HP ProtectTools
ユーザ ガイド

初版：2008 年 6 月

製品番号：481201-291

目次

5 File Sanitizer for HP ProtectTools

6 BIOS Configuration for HP ProtectTools

7 Embedded Security for HP ProtectTools（一部のモデルのみ）

8 Device Access Manager for HP ProtectTools（一部のモデルのみ）

9 トラブルシューティング

1 セキュリティの概要

HP ProtectTools セキュリティ マネージャ ソフトウェアは、コンピュータ本体、ネットワーク、および重要なデータを不正なアクセスから保護するために役立つセキュリティ機能を提供します。以下のソフトウェア モジュールによって、高度なセキュリティ機能が提供されます。

- Credential Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools（一部のモデルのみ）
- Privacy Manager for HP ProtectTools（一部のモデルのみ）
- File Sanitizer for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Embedded Security for HP ProtectTools（一部のモデルのみ）
- Device Access Manager for HP ProtectTools（一部のモデルのみ）

コンピュータで利用可能なソフトウェア モジュールは、モデルによって異なる可能性があります。たとえば、Embedded Security for HP ProtectTools は、TPM（Trusted Platform Module）セキュリティ チップが内蔵されているコンピュータでのみ使用できます。

HP ProtectTools ソフトウェア モジュールは、プリインストールまたはプリロードされている場合と、HP の Web サイトからダウンロードできる場合があります。詳しくは、http://www.hp.com/jp/にアクセスしてください。

注記： このガイドの操作手順は、該当する HP ProtectTools ソフトウェア モジュールがすでにインストールされていることを前提に書かれています。

HP ProtectTools の機能

以下の表で、HP ProtectTools モジュールの主な機能を詳しく説明します。

モジュール	主な機能
Credential Manager for HP ProtectTools	● Credential Manager には、個人のパスワードを保管できます。ユーザの証明情報を自動的に記憶して適用するシングルサインオン機能を使用してログオン プロセスを効率化します ● また、シングルサインオンは、ユーザ認証に Java™Card や指紋認証などの異なるセキュリティ テクノロジの組み合わせを要求することによって、さらなる保護機能を提供します ● パスワード記憶域はソフトウェアによる暗号化によって保護されており、TPM（Trusted Platform Module）内蔵セキュリティ チップ、または Java Card や指紋認証などのセキュリティ デバイス認証を使用することによって強化できます
Drive Encryption for HP ProtectTools（一部のモデルのみ）	● Drive Encryption では、ボリューム全体にわたる完全なハードドライブの暗号化が可能です ● Drive Encryption では、データの暗号化解除やデータへのアクセスにブート前認証が強制されます
Privacy Manager for HP ProtectTools（一部のモデルのみ）	● Privacy Manager は、電子メール、Microsoft® Office ドキュメント、またはインスタント メッセージ（IM）を使用するときに、高度なログオン技術を利用して、通信の発信元、整合性、セキュリティを確認します
File Sanitizer for HP ProtectTools	● File Sanitizer を使用すると、コンピュータ上のデジタル資産（アプリケーション ファイル、履歴コンテンツや Web 関連コンテンツ、その他の機密データなどの機密情報）を安全にシュレッドしたり、ハードドライブを定期的に「ブリーチ（漂白）」したりすることができます
BIOS Configuration for HP ProtectTools	● BIOS Configuration を使用すると、電源投入時のユーザおよび管理者パスワードの管理機能にアクセスできます ● BIOS Configuration は、[Computer Setup]と呼ばれる、ブート前 BIOS コンフィギュレーション ユーティリティの代わりに使用できます ● BIOS Configuration の内蔵セキュリティ チップで機能強化された自動 DriveLock（ドライブ ロック）の実現によって、ハードドライブがシステムから取り外されている場合でも、ハードドライブを不正なアクセスから保護することができます。ユーザは、内蔵セキュリティ チップのユーザ パスワード以外のパスワードを記憶する必要がありません

モジュール	主な機能
Embedded Security for HP ProtectTools（一部のモデルのみ）	● Embedded Security は、TPM（Trusted Platform Module）内蔵セキュリティ チップを使用して、コンピュータ本体に保存されている機密のユーザ データまたは証明情報を不正なアクセスから保護するために役立ちます ● Embedded Security を使用すると、ユーザのファイルおよびフォルダ情報を保護するのに役立つ PSD（Personal Secure Drive）を作成できます ● Embedded Security は、保護されたデジタル証明情報の操作のための他社製のアプリケーション（Microsoft Outlook や Internet Explorer など）をサポートします
Device Access Manager for HP ProtectTools（一部のモデルのみ）	● Device Access Manager を使用すると、IT 管理者は、ユーザ プロファイルに基づいてデバイスへのアクセスを制御できます ● Device Access Manager は、不正なユーザが外部のストレージ メディアを使用してデータを削除したり、外部のメディアからシステムにウィルスを侵入させたりできないようにします ● 管理者は、特定の個人またはユーザのグループに対して、書き込み可能なデバイスへのアクセスを無効にすることができます

HP ProtectTools セキュリティへのアクセス

Windows®の[コントロール パネル]から HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャ）にアクセスするには、以下の手順で操作します。

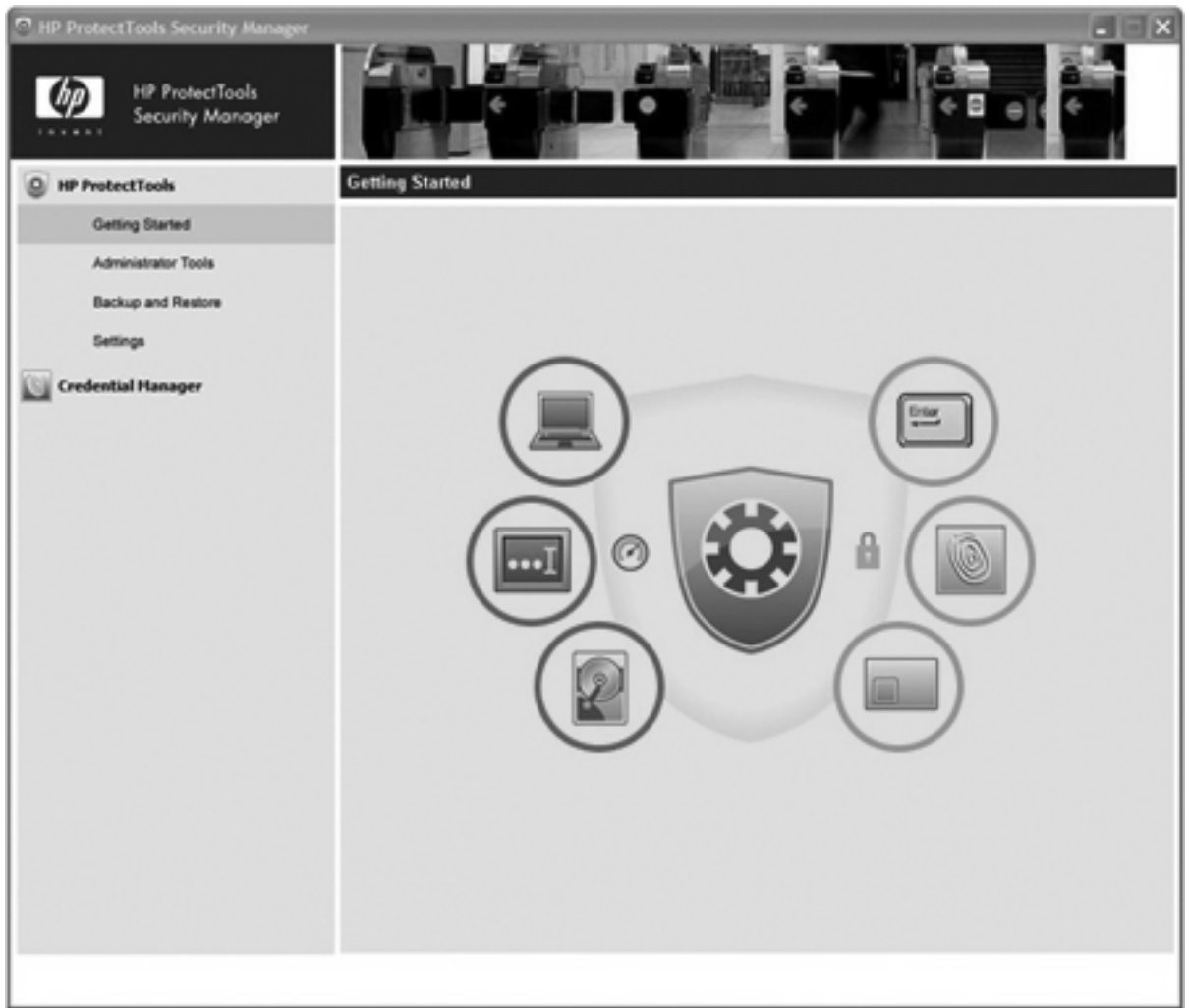
1. Windows Vista® をお使いの場合は、**[スタート]→[HP ProtectTools Security Manager for Administrators]**（管理者用 HP ProtectTools セキュリティ マネージャ）の順にクリックします。

   または

   Windows XP をお使いの場合は、**[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。

   注記： HP ProtectTools 管理者でない場合、管理者以外のモードで HP ProtectTools を実行して情報を表示することはできますが、変更を加えることはできません。

2. 左側のパネルで、**[HP ProtectTools]→[Getting Started]**（ここから開始）の順にクリックします。
3. HP ProtectTools のシールドアイコンの真下にある**[Security Manager Setup]**（セキュリティ マネージャのセットアップ）ボタンをクリックして、Security Manager（セキュリティ マネージャ）のウィザードを起動します。

   次のページが表示されます。

- Windows オペレーティング システム管理者は、ウィザードの説明に沿って、Credential Manager および Drive Encryption のブート前環境で使用されるセキュリティのレベルおよびセキュリティ ログオン方法を設定できます。
- ユーザも、セットアップ ウィザードを使用してセキュリティ ログオン方法を設定します。

注記： 各 HP ProtectTools モジュールにアクセスして強力な機能をセットアップするには、モジュール アイコンをクリックします。

注記： Credential Manager モジュールを設定した後は、Windows のログオン画面から直接 Credential Manager にログオンして HP ProtectTools を起動することもできます。詳しくは、17 ページの「Credential Manager を使用した Windows へのログオン」を参照してください。

主なセキュリティの目的の実現

各 HP ProtectTools モジュールが連携して動作することによって、以下の主なセキュリティの目的を含む、さまざまなセキュリティの問題に対処するためのソリューションを提供できます。

- 盗難からの保護
- 機密データへのアクセス制限
- 内部または外部からの不正なアクセスの防止
- 強力なパスワード ポリシーの作成
- セキュリティを義務付ける規制への対応

盗難からの保護

盗難の例として、空港の検問所での、機密データや顧客情報を含むコンピュータの盗難が挙げられます。盗難からの保護には、以下の機能が役立ちます。

- ブート前認証機能が有効になっていると、オペレーティング システムへのアクセスの防止に役立ちます。以下の項目を参照してください。
  - Credential Manager
  - Embedded Security
  - Drive Encryption
- DriveLock（ドライブロック）は、ハードドライブが取り外されて、セキュリティ保護されていないシステムに取り付けられている場合でもデータにアクセスできないようにするために役立ちます。
- Embedded Security for HP ProtectTools モジュールで提供される Personal Secure Drive 機能では、機密データを暗号化して、認証なしではアクセスできないようにします。以下の項目を参照してください。
  - 75 ページの 「セットアップ手順」（内蔵セキュリティのセットアップ）
  - 78 ページの 「PSD（Personal Secure Drive）の使用」

機密データへのアクセス制限

契約検査官がオンサイトで作業しており、機密の財務データの確認のためにコンピュータへのアクセスを許可されているとします。ただし、この検査官がこれらのファイルを印刷したり、CD などの書き込み可能なデバイスに保存できるようにはしたくありません。データへのアクセスを制限するには、以下の機能が役立ちます。

- Device Access Manager for HP ProtectTools を使用すると、IT 管理者は、機密情報を印刷したり、ハードドライブからリムーバブル メディアにコピーしたりできないように、書き込み可能なデバイスへのアクセスを制限することができます。85 ページの 「デバイス クラス構成（詳細設定）」を参照してください。
- DriveLock（ドライブロック）は、ハードドライブが取り外されて、セキュリティ保護されていないシステムに取り付けられている場合でもデータにアクセスできないようにするために役立ちます。

内部または外部からの不正なアクセスの防止

セキュリティ保護されていない PC への不正なアクセスは、金融サービス、役員、または研究開発チームからのデータなどの社内ネットワーク リソースや、患者記録や個人の財務データなどの個人情報を非常に大きなリスクにさらすことになります。不正なアクセスを防止するには、以下の機能が役立ちます。

- ブート前認証機能が有効になっていると、オペレーティング システムへのアクセスの防止に役立ちます。以下の項目を参照してください。
    - Credential Manager
    - Embedded Security
    - Drive Encryption
- Embedded Security for HP ProtectTools は、以下の方法で、コンピュータ本体に保存されている機密のユーザ データまたは証明情報を保護するために役立ちます。
    - 75 ページの 「セットアップ手順」（内蔵セキュリティのセットアップ）
    - 78 ページの 「PSD（Personal Secure Drive）の使用」
- Credential Manager for HP ProtectTools は、以下方法で、不正なユーザがパスワードを入手したり、パスワードで保護されたアプリケーションにアクセスしたりできないようにするために役立ちます。
    - 12 ページの 「セットアップ手順」（Credential Manager のセットアップ）
    - 18 ページの 「シングルサインオンの使用」
- Device Access Manager for HP ProtectTools を使用すると、IT 管理者は、機密情報をハードドライブからコピーできないように、書き込み可能なデバイスへのアクセスを制限することができます。84 ページの 「簡易構成」を参照してください。
- Personal Secure Drive 機能では、以下の方法で機密データを暗号化し、認証なしではアクセスできないようにします。
    - 75 ページの 「セットアップ手順」（内蔵セキュリティのセットアップ）
    - 78 ページの 「PSD（Personal Secure Drive）の使用」

強力なパスワード ポリシーの作成

いくつもの Web ベースのアプリケーションやデータベースに対して強力なパスワード ポリシーを使用する必要が生じた場合、Credential Manager for HP ProtectTools で以下の方法によって、パスワードやシングルサインオンのための保護されたリポジトリが提供されます。

- 12 ページの 「セットアップ手順」（Credential Manager のセットアップ）
- 18 ページの 「シングルサインオンの使用」

セキュリティを強化するために、Embedded Security for HP ProtectTools は、次にユーザ名とパスワードのリポジトリを保護します。これによって、ユーザはメモに残したり覚えたりしなくても、複数の強力なパスワードを保持することができます。75 ページの 「セットアップ手順」（Embedded Security のセットアップ）を参照してください。

その他のセキュリティ対策

セキュリティの役割の割り当て

コンピュータのセキュリティを（特に、大きな組織で）管理する上では、責任および権限をさまざまな管理者やユーザに割り当てることが重要な作業の 1 つです。

注記： 小さな組織や個人で使用する場合などは、一人の人がすべての役割を受け持つこともできます。

HP ProtectTools では、セキュリティの責任および権限を以下のように分けられます。

- セキュリティ統括責任者：企業またはネットワークのセキュリティ レベルを定義し、Java™ Cards、指紋認証システム、USB トークンなど、配備するセキュリティ機能を決定します。

  注記： HP ProtectTools の機能の多くは、セキュリティ統括責任者が HP と協力してカスタマイズできます。詳しくは、HP の Web サイト http://www.hp.com/jp/を参照してください。

- IT 管理者：セキュリティ統括責任者によって定義されたセキュリティ機能を適用し、管理します。また、一部の機能を有効または無効にできます。たとえば、セキュリティ統括責任者が Java Card の配備を決定した場合、IT 管理者は Java Card の BIOS セキュリティ モードを有効にすることができます。
- ユーザ：セキュリティ機能を使用します。たとえば、セキュリティ統括責任者および IT 管理者がシステムで Java Card を有効にしている場合、ユーザは Java Card の PIN を設定し、そのカードを認証に使用できます。

HP ProtectTools のパスワードの管理

HP ProtectTools セキュリティ マネージャの機能のほとんどは、パスワードによってセキュリティ保護されています。以下の表に、よく使用されるパスワード、そのパスワードが設定されるソフトウェア モジュール、およびパスワード機能の一覧を示します。

この表には、IT 管理者のみが設定して使用するパスワードも示されています。その他のすべてのパスワードは、一般のユーザまたは管理者が設定できます。

HP ProtectTools のパスワード	設定する HP ProtectTools モジュール	機能
Credential Manager のログオン パスワード	Credential Manager	このパスワードには、以下の 2 つのオプションがあります • Windows にログオンした後、Credential Manager にアクセスするための別のログオンで使用できます • Windows ログオン プロセスの代わりに使用し、Windows と Credential Manager に同時にアクセスできます
Credential Manager リカバリ ファイルのパスワード	Credential Manager、IT 管理者が設定	Credential Manager リカバリ ファイルへのアクセスを保護します
基本ユーザ キーのパスワード **注記：** 内蔵セキュリティ パスワードとも呼ばれます	Embedded Security	安全な電子メール、ファイル、およびフォルダの暗号化など Embedded Security 機能へのアクセスに使用します。電源投入時認証に使用すると、コンピュータの起動時や再起動時、またはハイバネーションからの

HP ProtectTools のパスワード	設定する HP ProtectTools モジュール	機能
		復帰時にコンピュータのデータを保護します
緊急リカバリ トークンのパスワード **注記：** 緊急リカバリ トークン キーのパスワードとも呼ばれます	Embedded Security、IT 管理者が設定	内蔵セキュリティ チップ用のバックアップ ファイルである緊急リカバリ トークンへのアクセスを保護します
所有者のパスワード	Embedded Security、IT 管理者が設定	システムと TPM（Trusted Platform Module）チップを、Embedded Security のすべての所有者機能への不正なアクセスから保護します
Java™ Card の PIN	Java Card Security	Java Card の内容へのアクセスを保護し、Java Card のユーザを認証します。電源投入時認証に使用すると、Java Card の PIN の入力によって[Computer Setup]ユーティリティおよびコンピュータのデータも保護されます Java Card トークンが選択されている場合は、Drive Encryption のユーザを認証します
[Computer Setup]のパスワード **注記：** BIOS の管理者パスワード、f10 セットアップ パスワード、またはセキュリティ セットアップ パスワードとも呼ばれます	BIOS Configuration、IT 管理者が設定	[Computer Setup]ユーティリティへのアクセスを保護します
Power-on Password（電源投入時パスワード）	BIOS Configuration	コンピュータの起動時や再起動時、またはハイバネーションからの復帰時にコンピュータのデータを保護します
Windows のログオン パスワード	Windows の[コントロール パネル]	手動ログオンで使用するか、または Java Card に保存できます

安全なパスワードの作成

パスワードを作成する場合は、まず、プログラムで設定されている仕様に従う必要があります。ただし一般的には、強力なパスワードを作成し、そのパスワードが危険にさらされないようにするために、以下のガイドラインを考慮してください。

- 文字数が 6 文字、できれば 8 文字を超えるパスワードを使用します。
- パスワード全体にわたって大文字と小文字を混在させます。
- 可能な場合は、常に半角アルファベットと半角数字を混在させ、さらに特殊文字と句読点を含めます。
- パスワード中の文字の代わりに特殊文字または数字を使用します。たとえば、アルファベットの l または L の代わりに数字の 1 を使用します。
- 2 つ以上の言語から取った単語を組み合わせます。
- 単語またはフレーズを数字や特殊文字で分割します。たとえば、「Mary2-2Cat45」とします。
- 辞書に載っているような用語は使用しないでください。
- 名前やその他の個人情報（たとえば、誕生日、ペットの名前、母親の旧姓など）は、たとえ綴りを逆にしたとしても、パスワードには使用しないでください。
- パスワードは定期的に変更してください。いくつかの文字や数字をその次の値に変更するだけでも構いません。
- パスワードをメモした場合は、コンピュータのすぐ近くの、人目につきやすい場所に保管しないでください。
- パスワードを、電子メールなどのコンピュータ上のファイルに保存しないでください。
- アカウントを共有したり、パスワードを誰かに教えたりしないでください。

HP ProtectTools 証明情報のバックアップおよび復元

サポートされているすべての HP ProtectTools モジュールからの証明情報をバックアップおよび復元するには、以下を参照してください。

証明情報および設定のバックアップ

以下の方法で証明情報をバックアップできます。

- Drive Encryption for HP ProtectTools を使用して、HP ProtectTools 証明情報の選択およびバックアップを行う

  オンラインの Drive Encryption キー復元サービスに登録して、暗号化キーのバックアップ コピーを保管することもできます。これによって、パスワードを忘れてしまい、ローカル バックアップにアクセスできない場合でも、コンピュータにアクセスすることができます。

  注記： このサービスを使用してパスワードを登録し、復元するには、コンピュータがインターネットに接続されていること、およびユーザが有効な電子メール アドレスを持っていることが必要です。

- Embedded Security for HP ProtectTools を使用して、HP ProtectTools 証明情報をバックアップする

2 Credential Manager for HP ProtectTools

Credential Manager for HP ProtectTools では、以下のセキュリティ機能を使用して、コンピュータを不正なアクセスから保護します。

- Windows へのログオン時のパスワードに代わる、Java Card や指紋認証システムなどを使用した Windows へのログオン。詳しくは、12 ページの 「証明情報の登録」を参照してください。
- Web サイト、アプリケーション、および保護されたネットワーク リソースでの証明情報を自動的に記憶するシングルサインオン機能。
- Java Card や指紋認証システムなどの、オプションのセキュリティ デバイスのサポート。
- コンピュータのロック解除にはオプションのセキュリティ デバイスを使用した認証を必要とするなどの、追加のセキュリティ設定のサポート。

セットアップ手順

Credential Manager へのログオン

設定に応じて、以下のどれかの方法で Credential Manager にログオンできます。

- 通知領域の[HP ProtectTools Security Manager]（HP ProtectTools セキュリティ マネージャ）アイコン
- Windows Vista をお使いの、**[スタート]**→**[HP ProtectTools Security Manager for Administrators]**（管理者用 HP ProtectTools セキュリティ マネージャ）の順にクリックします。
- Windows XP をお使いの場合は、**[スタート]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。

注記： Windows Vista をお使いの場合は、変更を加えるには[HP ProtectTools Security Manager for Administrators]（管理者用 HP ProtectTools セキュリティ マネージャ）を起動する必要があります。

Credential Manager にログオンした後、指紋や Java Card などの追加の証明情報を登録できます。詳しくは、12 ページの 「証明情報の登録」を参照してください。

次回のログオン時には、ログオン ポリシーを選択して、登録された証明情報の任意の組み合わせを使用することができます。

[Credential Manager Logon Wizard]（証明情報マネージャ ログオン ウィザード）の使用

[Credential Manager Logon Wizard]を使用して Credential Manager にログオンするには、以下の手順で操作します。

1. 以下のどれかの方法で[Credential Manager Logon Wizard]を起動します。
   - Windows のログオン画面を使用する
   - 通知領域から、**[HP ProtectTools Security Manager]**アイコンをダブルクリックする
   - HP ProtectTools セキュリティ マネージャの[Credential Manager]（証明情報マネージャ）ページから、ウィンドウの右上隅にある**[Log On]**（ログオン）リンクをクリックする
2. 画面の説明に沿って操作し、Credential Manager にログオンします。

証明情報の登録

[My Identity]（個人 ID）ページを使用して、各種の認証方法、または証明情報を登録できます。登録が完了した後、それらの方法を使用して Credential Manager にログオンできます。

指紋の登録

指紋認証システムでは、Windows パスワードではなく、指紋を使用して認証することで Windows にログオンできます。

指紋認証システムのセットアップ

1. HP ProtectTools セキュリティ マネージャで、左側のパネルの**[Credential Manager]**（証明情報マネージャ）をクリックします。
2. **[My Identity]**（個人 ID）→**[Register Fingerprints]**（指紋の登録）の順にクリックします。
3. 画面の説明に沿って操作し、指紋の登録と指紋認証システムのセットアップを完了します。
4. 別の Windows ユーザ用の指紋を登録するには、そのユーザとして Windows にログオンして上記の手順を繰り返します。

登録された指紋を使用した Windows へのログオン

1. 指紋を登録したらすぐに Windows を再起動します。
2. Windows の[ようこそ]画面で、登録された指のどれかを押し当てて Windows にログオンします。

スマート カードまたはトークンの登録

スマート カードは、情報をロードできるマイクロチップが埋め込まれた、ほぼクレジット カード サイズのプラスチック製カードです。スマート カードは、個々のユーザに対して情報の保護および認証を提供します。スマート カードを使用したネットワークへのログオンでは、ドメインに対してユーザを認証するときに暗号法ベースの識別と所有の証明を使用して、強力な形式の認証を提供することができます。

USB トークンは、異なるフォーム ファクタのスマート カードです。プラスチック製のクレジット プラットフォームにスマート チップを配備する代わりに、スマート チップが USB キーとも呼ばれるプラスチック製のトークンに挿入されます。スマート カードとトークンの主な違いは、アクセス インタフェースにあります。カードはリーダーを必要としますが、トークンは USB コネクタに直接差し込みます。証明情報を保管および提供するためのコア機能には違いはありません。

USB トークンは、強力な認証に使用されます。拡張セキュリティを提供し、安全な情報アクセスを保証します。

注記： この手順を実行するには、カード リーダーを設定しておく必要があります。リーダーが装備されていない場合は、15 ページの「仮想トークンの作成」の説明に沿って仮想トークンを登録できます。

1. HP ProtectTools セキュリティ マネージャで、左側のパネルの**[Credential Manager]**（証明情報マネージャ）をクリックします。
2. **[My Identity]**（個人 ID）→**[Register Smart Card or Token]**（スマート カードまたはトークンの登録）の順にクリックします。
3. **[Device Type]**（デバイスの種類）ダイアログ ボックスで、目的のデバイスの種類をクリックし、**[Next]**（次へ）をクリックします。
4. デバイスの種類としてスマート カードまたは USB トークンが選択された場合は、スマート カードが挿入されている、またはトークンが USB コネクタに接続されていることを確認します。

   注記： スマート カードが挿入されていない、または USB トークンが接続されていない場合、[Select Token]（トークンの選択）ダイアログ ボックスの[Next]ボタンは無効です。

5. [Device Type]ダイアログ ボックスで、**[Next]**（次へ）を選択します。

[Token Properties]（トークンのプロパティ）ダイアログ ボックスが表示されます。

6. ユーザ PIN を入力し、**[Register smart card or token for authentication]**（認証用のスマートカードまたはトークンの登録）を選択し、**[Finish]**（完了）をクリックします。

その他の証明情報の登録

1. HP ProtectTools セキュリティ マネージャで、**[Credential Manager]**（証明情報マネージャ）をクリックします。
2. **[My Identity]**（個人 ID）→**[Register Credentials]**（証明情報の登録）の順にクリックします。

   [Credential Manager Registration Wizard]（証明情報マネージャ登録ウィザード）が起動します。
3. 画面に表示される説明に沿って操作します。

一般的なタスク

Credential Manager の[My Identity]（個人 ID）ページには、すべてのユーザがアクセスできます。[My Identity]ページから、以下のことができます。

- Windows ログオン パスワードの変更
- トークン PIN の変更
- ワークステーションのロック

注記： このオプションは、Credential Manager のクラシック ログオン画面が有効に設定されている場合にのみ利用できます。25 ページの 「例 1：[Advanced Settings]（詳細設定）ページを使用して、Credential Manager からの Windows ログオンを可能にする方法」を参照してください。

仮想トークンの作成

仮想トークンの機能は、Java Card や USB トークンとよく似ています。このトークンは、コンピュータのハードドライブ上か、Windows レジストリ内のどちらかに保存されます。仮想トークンでログオンすると、認証を完了するためにユーザ PIN の入力を要求されます。

新しい仮想トークンを作成するには、以下の手順で操作します。

1. HP ProtectTools セキュリティ マネージャで、左側のパネルの**[Credential Manager]**（証明情報マネージャ）をクリックします。
2. **[My Identity]**（個人 ID）→**[Register Smart Card or Token]**（スマート カードまたはトークンの登録）の順にクリックします。
3. **[Device Type]**（デバイスの種類）ダイアログ ボックスで、**[Virtual Token]**（仮想トークン）をクリックし、**[Next]**（次へ）をクリックします。
4. トークン名と場所を指定し、**[Next]**（次へ）をクリックします。

   新しい仮想トークンは、ファイルまたは Windows レジストリ データベースに保管できます。
5. [Token Properties]（トークンのプロパティ）ダイアログ ボックスで、新しく作成された仮想トークンのマスタ PIN とユーザ PIN を指定し、**[Register smart card or token for authentication]**（認証用のスマート カードまたはトークンの登録）をクリックし、**[Finish]**（完了）をクリックします。

Windows ログオン パスワードの変更

1. HP ProtectTools セキュリティ マネージャで、左側のパネルの**[Credential Manager]**（証明情報マネージャ）をクリックします。
2. **[My Identity]**（個人 ID）→**[Change Windows Password]**（Windows パスワードの変更）の順にクリックします。
3. **[Old password]**（古いパスワード）ボックスに、古いパスワードを入力します。
4. **[New Password]**（新しいパスワード）ボックスおよび**[Confirm password]**（パスワードの確認）ボックスに新しいパスワードを入力します。
5. **[Finish]**（完了）をクリックします。

トークン PIN の変更

1. HP ProtectTools セキュリティ マネージャで、左側のパネルの**[Credential Manager]**（証明情報マネージャ）をクリックします。
2. **[My Identity]**（個人 ID）→**[Change Token PIN]**（トークン PIN の変更）の順にクリックします。
3. [Device Type]（デバイスの種類）ダイアログ ボックスで、目的のデバイスの種類をクリックし、**[Next]**（次へ）をクリックします。
4. PIN を変更するトークンを選択して**[Next]**（次へ）をクリックします。
5. 画面の説明に沿って操作し、PIN の変更を完了します。

注記： 誤った PIN を数回連続して入力すると、トークンはロックされます。ロックを解除するまで、このトークンを使用することはできません。

コンピュータ（作業環境）のロック

この機能は、Credential Manager を使用して Windows にログオンした場合に利用できます。席を離れている間のコンピュータの安全を確保するには、作業環境のロック機能を使用します。これによって、不正なユーザによるコンピュータへのアクセスを防ぐことができます。このロックは、自分自身と、コンピュータ上の管理者グループのメンバのみが解除できます。

注記： このオプションは、Credential Manager のクラシック ログオン画面が有効に設定されている場合にのみ利用できます。25 ページの 「例 1：[Advanced Settings]（詳細設定）ページを使用して、Credential Manager からの Windows ログオンを可能にする方法」を参照してください。

コンピュータのロック解除に Java Card、指紋認証システム、またはトークンが必要となるように作業環境のロック機能を設定することで、セキュリティを強化できます。詳しくは、25 ページの「Credential Manager の設定」を参照してください。

1. HP ProtectTools セキュリティ マネージャで、左側のパネルの**[Credential Manager]**（証明情報マネージャ）をクリックします。
2. **[My Identity]**（個人 ID）をクリックします。
3. **[Lock Workstation]**（作業環境をロック）をクリックしてコンピュータをただちにロックします。

   コンピュータのロックを解除するには、Windows パスワードまたは[Credential Manager Logon Wizard]（証明情報マネージャ ログオン ウィザード）を使用する必要があります。

Windows のログオンの使用

ローカル コンピュータまたはネットワーク ドメインのどちらでも、Credential Manager を使用して Windows にログオンできます。初めて Credential Manager にログオンすると、ローカルの Windows ユーザ アカウントが Windows ログオン サービス用のアカウントとして自動的に追加されます。

Credential Manager を使用した Windows へのログオン

Credential Manager を使用して、Windows のネットワークまたはローカル アカウントにログオンできます。

1. Windows へのログオン用に指紋を登録してある場合は、指を押し当ててログオンします。
2. Windows XP をお使いの場合で、Windows へのログオン用に指紋を登録していない場合は、画面の左上隅にある指紋アイコンの隣のキーボード アイコンをクリックします。[Credential Manager Logon Wizard]（証明情報マネージャ ログオン ウィザード）が起動します。

   Windows Vista をお使いの場合で、Windows へのログオン用に指紋を登録していない場合は、ログオン画面の**[Credential Manager]**（証明情報マネージャ）をクリックします。[Credential Manager Logon Wizard]（証明情報マネージャ ログオン ウィザード）が起動します。
3. **[User name]**（ユーザ名）の矢印→自分の名前の順にクリックします。
4. **[Password]**（パスワード）ボックスにパスワードを入力して**[Next]**（次へ）をクリックします。

5. **[More]**（詳細）→**[Wizard Options]**（ウィザード オプション）の順に選択します。

   a. 次回コンピュータにログオンした時にこの名前を初期設定のユーザ名にする場合は、**[Use last user name on next logon]**（前回のユーザ名を次のログオン時に使用）チェック ボックスにチェックを入れます。

   b. このログオン ポリシーを初期設定の認証方法にする場合は、**[Use last policy on next logon]**（前回のポリシーを次のログオン時に使用）チェック ボックスにチェックを入れます。

6. 画面に表示される説明に沿って操作します。認証情報が正しい場合は、Windows アカウントおよび Credential Manager にログオンします。

シングルサインオンの使用

Credential Manager には、複数のインターネットおよび Windows プログラム用のユーザ名とパスワードを格納し、ユーザが登録されたプログラムにアクセスすると自動的にログオン証明情報を入力する、シングルサインオン機能があります。

注記： シングルサインオンの重要な機能は、セキュリティとプライバシです。証明情報はすべて暗号化されており、Credential Manager へのログオンに成功した後にのみ使用できます。

注記： セキュリティ保護されたサイトまたはプログラムにログオンする前に、Java Card、指紋認証システム、またはトークンを使用して認証証明情報を検証するように、シングルサインオンを設定することもできます。この機能は、銀行口座番号などの個人情報が含まれているプログラムまたは Web サイトにログオンする場合に特に有効です。詳しくは、25 ページの 「Credential Manager の設定」を参照してください。

新しいアプリケーションの登録

Credential Manager では、Credential Manager にログオンしている間に起動するアプリケーションをすべて登録するよう要求されます。アプリケーションを手動で登録することもできます。

自動登録の使用

1. ログオンが必要なアプリケーションを起動します。

2. プログラムまたは Web サイトのパスワード ダイアログ ボックスで[Credential Manager SSO]（証明情報マネージャ シングルサインオン）アイコンをクリックします。

3. プログラムまたは Web サイトのパスワードを入力して**[OK]**をクリックします。**[Credential Manager Single Sign On]**（証明情報マネージャ シングルサインオン）ダイアログ ボックスが開きます。

4. **[More]**（詳細）をクリックして以下のオプションのどれかを選択します。

   - [Do not use SSO for this site or application.]（このサイトまたはアプリケーションではシングルサインオン（SSO）を使用しない。）

   - [Prompt to select account for this application.]（このアプリケーションのアカウントの選択画面を表示する。）

   - [Fill in credentials but do not submit.]（証明情報を入力するが送信はしない。）

- [Authenticate user before submitting credentials.]（証明情報を送信する前にユーザ認証を行う。）
- [Show SSO shortcut for this application.]（このアプリケーションの SSO ショートカットを表示する。）

5. **[Yes]**（はい）をクリックして、登録を完了します。

手動（ドラッグ アンド ドロップ）登録の使用

1. HP ProtectTools セキュリティ マネージャの左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
2. **[Manage Services and Applications]**（サービスおよびアプリケーションの管理）をクリックします。

   Credential Manager Single Sign On（証明情報マネージャ シングルサインオン）ダイアログ ボックスが表示されます。
3. 以前に登録した Web サイトまたはアプリケーションを変更または削除するには、一覧で目的のレコードを選択します。
4. 画面に表示される説明に沿って操作します。

アプリケーションおよび証明情報の管理

アプリケーション プロパティの変更

1. HP ProtectTools セキュリティ マネージャの左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
2. **[Manage Services and Applications]**（サービスおよびアプリケーションの管理）をクリックします。

   Credential Manager Single Sign On（証明情報マネージャ シングルサインオン）ダイアログ ボックスが表示されます。
3. 変更するアプリケーション エントリをクリックして**[Properties]**（プロパティ）をクリックします。
4. **[General]**（全般）タブをクリックして、アプリケーション名および説明を変更します。該当する設定の横にあるチェック ボックスにチェックを入れるか外して、設定を変更します。
5. **[Script]**（スクリプト）タブをクリックして、SSO アプリケーション スクリプトを表示し、編集します。
6. **[OK]**をクリックします。

シングルサインオンからのアプリケーションの削除

1. HP ProtectTools セキュリティ マネージャの左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
2. **[Manage Services and Applications]**（サービスおよびアプリケーションの管理）をクリックします。

   Credential Manager Single Sign On（証明情報マネージャ シングルサインオン）ダイアログ ボックスが表示されます。
3. 削除するアプリケーション エントリをクリックして**[Remove]**（削除）をクリックします。
4. 確認ダイアログ ボックスで**[Yes]**（はい）をクリックします。
5. **[OK]**をクリックします。

アプリケーションのエクスポート

アプリケーションをエクスポートして、シングルサインオン アプリケーション スクリプトのバックアップ コピーを作成できます。このファイルは、後でシングルサインオン データの復元に使用できます。これは、証明情報のみが含まれている ID バックアップ ファイルを補うものとして機能します。

アプリケーションをエクスポートするには、以下の手順で操作します。

1. HP ProtectTools セキュリティ マネージャの左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
2. **[Manage Services and Applications]**（サービスおよびアプリケーションの管理）をクリックします。

   Credential Manager Single Sign On（証明情報マネージャ シングルサインオン）ダイアログ ボックスが表示されます。
3. エクスポートするアプリケーション エントリをクリックして**[More]**（詳細）をクリックします。
4. 画面の説明に沿って操作し、エクスポートを完了します。
5. **[OK]**をクリックします。

アプリケーションのインポート

1. HP ProtectTools セキュリティ マネージャの左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
2. **[Manage Services and Applications]**（サービスおよびアプリケーションの管理）をクリックします。

   Credential Manager Single Sign On（証明情報マネージャ シングルサインオン）ダイアログ ボックスが表示されます。
3. インポートするアプリケーション エントリをクリックして**[More]**（詳細）をクリックします。
4. 画面の説明に沿って操作し、インポートを完了します。
5. **[OK]**をクリックします。

証明情報の変更

1. HP ProtectTools セキュリティ マネージャで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
2. **[Manage Services and Applications]**（サービスおよびアプリケーションの管理）をクリックします。

   Credential Manager Single Sign On（証明情報マネージャ シングルサインオン）ダイアログ ボックスが表示されます。
3. 変更するアプリケーション エントリをクリックして**[More]**（詳細）をクリックします。
4. 以下のオプションのどれかを選択します。
   - Applications（アプリケーション）
     - Add New（新規追加）
     - Remove（削除）
     - Properties（プロパティ）
     - Import Script（スクリプトのインポート）
     - Export Script（スクリプトのエクスポート）
   - 証明情報
     - Create New（新規作成）
   - View Password（パスワードの表示）

   注記： パスワードを表示するには、事前に ID の認証を行う必要があります。
5. 画面に表示される説明に沿って操作します。
6. **[OK]**をクリックします。

アプリケーションの保護機能の使用

この機能を使用して、アプリケーションへのアクセス設定を行えます。以下の基準に基づいてアクセスを制限できます。

- ユーザのカテゴリ
- 使用する時間
- 無操作の状態

アプリケーションへのアクセス制限

1. HP ProtectTools セキュリティ マネージャの左側のパネルで、**[Credential Manager]**（証明情報マネージャ）→**[Services and Applications]**（サービスおよびアプリケーション）の順にクリックします。
2. **[アプリケーションの保護]**をクリックします。
3. アクセスを管理したいユーザのカテゴリを選択します。

注記： カテゴリが[Everyone]（全員）でない場合は、[Everyone]（全員）カテゴリ以外を優先させるために**[Override default settings]**（初期設定以外を優先する）を選択する必要が生じる場合があります。

4. **[Add]**（追加）をクリックします。

   [Add a Program Wizard]（プログラムの追加ウィザード）が起動します。

5. 画面に表示される説明に沿って操作します。

アプリケーションの保護の解除

アプリケーションのアクセス制限を解除するには、以下の手順で操作します。

1. HP ProtectTools セキュリティ マネージャで、左側のパネルの**[Credential Manager]**（証明情報マネージャ）をクリックします。

2. **[Services and Applications]**（サービスおよびアプリケーション）をクリックします。

3. **[Application Protection]**（アプリケーションの保護）をクリックします。

4. アクセスを管理したいユーザのカテゴリを選択します。

   注記： カテゴリが[Everyone]（全員）でない場合は、[Everyone]カテゴリ以外を優先させるために**[Override default settings]**（初期設定以外を優先する）をクリックする必要が生じる場合があります。

5. 削除するアプリケーション エントリをクリックして**[Remove]**（削除）をクリックします。

6. **[OK]**をクリックします。

保護されたアプリケーションの制限設定の変更

1. **[Application Protection]**（アプリケーションの保護）をクリックします。

2. アクセスを管理したいユーザのカテゴリを選択します。

   注記： カテゴリが[Everyone]（全員）でない場合は、[Everyone]カテゴリ以外を優先させるために**[Override default settings]**（初期設定以外を優先する）をクリックする必要が生じる場合があります。

3. 変更するアプリケーションをクリックして**[Properties]**（プロパティ）をクリックします。そのアプリケーションの**[Properties]**（プロパティ）ダイアログ ボックスが開きます。

4. **[General]**（全般）タブをクリックします。以下の設定のどれかを選択します。

   - [Disabled (Cannot be used)]（無効（使用不可））
   - [Enabled (Can be used without restrictions)]（有効（無制限に使用可能））
   - [Restricted (Usage depends on settings)]（制限あり（使用制限は設定によって異なる））

5. [Restricted]（制限あり）を選択した場合、以下の設定が利用可能になります。

   a. 時間、曜日、または日付に基づいて使用を制限する場合は、**[Schedule]**（スケジュール）タブをクリックして設定を行います。

   b. 無操作状態に基づいて使用を制限する場合は、**[Advanced]**（詳細）タブをクリックして無操作の期間を選択します。

6. **[OK]**をクリックして、アプリケーションの**[Properties]**ダイアログ ボックスを閉じます。
7. **[OK]**をクリックします。

高度なタスク（管理者のみ）

Credential Manager の[Authentication and Credentials]（認証および証明情報）ページおよび[Advanced Settings]（詳細設定）ページは、管理者権限を持つユーザのみが使用できます。これらのページから、以下のタスクを実行できます。

- ユーザおよび管理者のログオン方法の指定
- カスタム認証要件の設定
- 証明情報のプロパティの設定
- Credential Manager の設定

ユーザおよび管理者のログオン方法の指定

[Authentication and Credentials]（認証および証明情報）ページで、ユーザまたは管理者のどちらかに、どのような種類または組み合わせの証明情報が必要かを指定できます。

ユーザまたは管理者のログオン方法を指定するには、以下の手順で操作します。

1. HP ProtectTools セキュリティ マネージャで、左側のパネルの**[Credential Manager]**（証明情報マネージャ）をクリックします。
2. **[Multifactor Authentication]**（多元的な認証）をクリックします。
3. 右側のパネルで、**[Authentication]**（認証）タブをクリックします。
4. カテゴリの一覧から、カテゴリ（**[Users]**（ユーザ）または**[Administrators]**（管理者））をクリックします。
5. 一覧から、認証方法の種類または組み合わせをクリックします。
6. **[Apply]**（適用）→**[OK]**の順にクリックします。

カスタム認証要件の設定

[Authentication and Credentials]（認証および証明情報）ページの[Authentication]（認証）タブに、必要な認証証明情報のセットが一覧表示されない場合は、カスタム要件を作成できます。

カスタム要件を設定するには、以下の手順で操作します。

1. HP ProtectTools セキュリティ マネージャで、左側のパネルの**[Credential Manager]**（証明情報マネージャ）をクリックします。
2. **[Multifactor Authentication]**（多元的な認証）をクリックします。
3. 右側のパネルで、**[Authentication]**（認証）タブをクリックします。
4. カテゴリの一覧から、カテゴリ（**[Users]**（ユーザ）または**[Administrators]**（管理者））をクリックします。
5. 認証方法の一覧から、**[Custom]**（カスタム）をクリックします。
6. **[Configure]**（設定）をクリックします。
7. 使用する認証方法を選択します。
8. 以下のどちらかの項目をクリックして、方法の組み合わせを選択します。
   - AND を使用して認証方法を組み合わせる

     （ユーザはログオンするたびに、チェックを入れたすべての方法で認証する必要があります）
   - OR を使用して複数の認証方法のうち 1 つを要求する

     （ユーザはログオンするたびに、チェックを入れた方法のどれかを選択できます）
9. **[OK]**をクリックします。
10. **[Apply]**（適用）→**[OK]**の順にクリックします。

証明情報のプロパティの設定

[Authentication and Credentials]（認証および証明情報）ページの[Credentials]（証明情報）タブで、使用可能な認証方法の一覧を表示して設定を変更できます。

証明情報を設定するには、以下の手順で操作します。

1. HP ProtectTools セキュリティ マネージャで、左側のパネルの**[Credential Manager]**（証明情報マネージャ）をクリックします。
2. **[Multifactor Authentication]**（多元的な認証）をクリックします。
3. **[Credentials]**（証明書）タブをクリックします。

4. 変更する証明情報の種類をクリックします。以下のどれかの方法で証明情報を変更できます。
   - 証明情報を登録するには、**[Register]**（登録）をクリックし、画面の説明に沿って操作します。
   - 証明情報を削除するには、**[Clear]**（クリア）をクリックし、確認ダイアログ ボックスで**[Yes]**（はい）をクリックします。
   - 証明情報のプロパティを変更するには、**[Properties]**（プロパティ）をクリックし、画面の説明に沿って操作します。
5. **[Apply]**（適用）→**[OK]**の順にクリックします。

Credential Manager の設定

[Advanced Settings]（詳細設定）ページから、以下のタブを使用して各種の設定にアクセスし、変更することができます。

- General（全般）：基本的な設定を変更できます。
- Single Sign On（シングルサインオン）：現在のユーザに対するシングルサインオンの動作方法の設定（たとえば、ログオン画面の検出、登録されたログオン ダイアログへの自動ログオン、パスワードの表示などの処理方法）を変更できます。
- Services and Applications（サービスおよびアプリケーション）：使用可能なサービスを表示して、それらのサービスの設定を変更できます。
- Security（セキュリティ）：指紋認証ソフトウェアを選択して、指紋認証システムのセキュリティ レベルを調整できます。
- Smart Cards and Tokens（スマート カードおよびトークン）：使用可能なすべての Java Card およびトークンのプロパティを表示して変更できます。

Credential Manager の設定を変更するには、以下の手順で操作します。

1. HP ProtectTools セキュリティ マネージャで、左側のパネルの**[Credential Manager]**（証明情報マネージャ）をクリックします。
2. **[Settings]**（設定）をクリックします。
3. 変更する設定が含まれるタブをクリックします。
4. 画面の説明に沿って操作し、設定を変更します。
5. **[Apply]**（適用）→**[OK]**の順にクリックします。

例 1：[Advanced Settings]（詳細設定）ページを使用して、Credential Manager からの Windows ログオンを可能にする方法

1. HP ProtectTools セキュリティ マネージャで、左側のパネルの**[Credential Manager]**（証明情報マネージャ）をクリックします。
2. **[Settings]**（設定）をクリックします。
3. **[General]**（全般）タブをクリックします。
4. **[Select the way users log on to Windows (requires restart)]**（ユーザが Windows へログオンする方法の選択（再起動が必要））で、**[Use Credential Manager with classic logon prompt]**

（証明情報マネージャでクラシック ログオン画面を使用する）チェック ボックスにチェックを入れます。

5. **[Apply]**（適用）→**[OK]**の順にクリックします。

6. コンピュータを再起動します。

注記： **[Use Credential Manager with classic logon prompt]**（証明情報マネージャでクラシック ログオン画面を使用する）チェック ボックスにチェックを入れると、コンピュータをロックできるようになります。17 ページの 「コンピュータ（作業環境）のロック」を参照してください。

例 2：[Advanced Settings]（詳細設定）ページを使用して、シングルサインオンの前にユーザ確認を要求する方法

1. HP ProtectTools セキュリティ マネージャで、**[Credential Manager]**（証明情報マネージャ）→**[Settings]**（設定）の順にクリックします。

2. **[Single Sign On]**（シングルサインオン）タブをクリックします。

3. **[When registered logon dialog or Web page is visited]**（登録したログオン ダイアログまたは Web ページが表示された時の動作）で、**[Authenticate user before submitting credentials]**（証明情報を送信する前にユーザの認証を行う）チェック ボックスにチェックを入れます。

4. **[Apply]**（適用）→**[OK]**の順にクリックします。

5. コンピュータを再起動します。

3 Drive Encryption for HP ProtectTools（一部のモデルのみ）

△ **注意：** Drive Encryption モジュールをアンインストールする場合は、まず、暗号化されたすべてのドライブの暗号化を解除する必要があります。そうしないと、Drive Encryption 復元サービスに登録していない限り、暗号化されたドライブ上のデータにアクセスできなくなります。Drive Encryption モジュールを再インストールしても、暗号化されたドライブにはアクセスできません。

セットアップ手順

Drive Encryption を開く

1. [スタート]→[すべてのプログラム]→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。
2. **[Drive Encryption]**（ドライブの暗号化）をクリックします。

一般的なタスク

Drive Encryption の有効化

Drive Encryption を有効にするには、HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャ）のセットアップ ウィザードを使用します。

Drive Encryption の無効化

Drive Encryption を無効にするには、HP ProtectTools Security Manager のセットアップ ウィザードを使用します。

Drive Encryption の有効化後のログイン

Drive Encryption が有効になり、ユーザ アカウントが登録された後でコンピュータを起動した場合、Drive Encryption のログオン画面からログインする必要があります。

注記： Windows 管理者が HP ProtectTools Security Manager（HP ProtectTools セキュリティ マネージャ）で[Pre-boot Security]（ブート前セキュリティ）を有効にしている場合は、Drive Encryption のログオン画面からではなく、コンピュータが起動した直後にコンピュータにログインします。

1. ユーザ名を選択し、Windows のパスワードまたは Java™ Card の PIN を入力するか、または登録した指を押し当てます。
2. **[OK]**をクリックします。

注記： Drive Encryption のログオン画面で復元キーを使用してログオンする場合は、Windows のログオン画面で Windows のユーザ名を選択し、パスワードを入力することも要求されます。

高度なタスク

Drive Encryption の管理（管理者のタスク）

[Encryption Management]（暗号化管理）ページでは、Windows 管理者は Drive Encryption の状態（有効または無効）を表示および変更し、コンピュータ上のすべてのハードドライブの暗号化の状態を表示できます。

TPM で保護されたパスワードの有効化（一部のモデルのみ）

HP ProtectTools の[Embedded Security]（内蔵セキュリティ）ツールを使用して、TPM（Trusted Platform Module）を有効にします。TPM を有効にした後、Drive Encryption のログオン画面からログインするには、Windows のユーザ名およびパスワードを入力する必要があります。

注記： パスワードは TPM セキュリティ チップで保護されているため、ハードドライブを別のコンピュータに移動すると、TPM 設定をそのコンピュータに移行しない限り、データにアクセスできなくなります。

1. HP ProtectTools の[Embedded Security]ツールを使用して、TPM を有効にします。
2. Drive Encryption を開き、**[Encryption Management]**（暗号化管理）をクリックします。
3. **[TPM-protected password]**（TPM で保護されたパスワード）チェック ボックスにチェックを入れます。

個々のドライブの暗号化または暗号化の解除

1. Drive Encryption を開き、**[Encryption Management]**（暗号化管理）をクリックします。
2. **[Change Encryption]**（暗号化の変更）をクリックします。
3. [Change Encryption]ダイアログ ボックスで、暗号化するか、暗号化を解除する各ハードドライブの横にあるチェック ボックスにチェックを入れるか、またはチェックを外して、**[OK]**をクリックします。

注記： ドライブの暗号化または暗号化解除が行われている間、現在のセッションで処理が完了するまでの残り時間が進行状況バーに表示されます。暗号化中にコンピュータをシャットダウンするか、スリープまたはハイバネーションを開始してから起動しなおした場合、残り時間の表示はリセットされますが、実際の暗号化は直前に停止した場所から再開されます。残り時間と進行状況の表示がすばやく進み、現在の進行状況が反映されます。

バックアップおよび復元（管理者のタスク）

[Recovery]（復元）ページでは、Windows 管理者は暗号化キーをバックアップし、復元することができます。

バックアップ キーの作成

△ 注意： バックアップ キーを含むストレージ デバイスは必ず安全な場所に保管してください。パスワードを忘れたり、Java Card を紛失したりした場合に、このデバイスがハードドライブにアクセスする唯一の方法となります。

1. Drive Encryption を開き、**[Recovery]**（復元）をクリックします。
2. **[Backup Keys]**（キーをバックアップする）をクリックします。

3. [Select Backup Disk]（バックアップ ディスクの選択）ページで、暗号化キーをバックアップするデバイスの名前をクリックし、**[Next]**（次へ）をクリックします。

4. 次に表示されるページの情報を確認してから、**[Next]**（次へ）をクリックします。

   選択したストレージ デバイスに暗号化キーが保存されます。

5. 確認ダイアログ ボックスが表示されたら、**[OK]**をクリックします。

オンライン復元の登録

オンライン Drive Encryption キー復元サービスによって、暗号化キーのバックアップ コピーを保存できます。パスワードを忘れたためローカルのバックアップ データにアクセスできない場合には、このバックアップ コピーを使用することでコンピュータにアクセスできます。

注記： このサービスを使用してパスワードを登録し、復元するには、コンピュータがインターネットに接続されていること、およびユーザが有効な電子メール アドレスを持っていることが必要です。

1. Drive Encryption を開き、**[Recovery]**（復元）をクリックします。

2. **[Register]**（登録）をクリックします。

3. 以下のオプションのどちらかをクリックします。

   - [I want to create a new recovery account for this PC]（このコンピュータ用に新しい復元アカウントを作成する）：オプションを選択した場合は、電子メール アドレスおよびその他の情報を入力し、**[Next]**（次へ）をクリックします。

   - [I want to add this PC to my existing web recovery account]（このコンピュータを既存の Web 復元アカウントに追加する）

4. パスワードの作成および確認を行い、セキュリティに関する質問を選択して回答を入力してから、**[Next]**（次へ）をクリックします。

   注記： 指定した電子メール アドレスにアカウントのアクティブ化コードが送信されます。

5. アクティブ化コードを入力し、**[Next]**（次へ）をクリックします。

6. コンピュータのシリアル番号を入力し、**[Next]**（次へ）をクリックします。

   注記： コンピュータのシリアル番号を確認するには、**[スタート]**→**[ヘルプとサポート]**の順にクリックします。

7. サブスクリプション クーポンを持っていない場合は、**[Click here to purchase coupons]**（クーポンを購入するにはここをクリック）リンクをクリックします。

   このリンクをクリックすると、SafeBoot の[Recovery Service]の Web サイトが表示されます。ウィザードは終了しないでください。

8. **[Purchase Coupon Codes]**（クーポン コードを購入）をクリックします。

9. お住まいの国または地域とコンピュータの種類を選択し、**[Start]**（開始）をクリックします。

10. 1 年間のサブスクリプション オプションまたは 3 年間のサブスクリプション オプションの隣の**[Buy]**（購入）をクリックします。

11. **[Checkout]**（精算）をクリックします。

12. 取引条件を読み、**[Accept]**（受諾する）をクリックします。

13. 課金情報を入力し、**[Continue]**（続行）をクリックします。

14. クレジット カード情報を入力し、**[Make Payment]**（支払）をクリックします。

15. クーポン コードを書き留め、ウィザードの[Account Activation]（アカウント有効化）ページに戻ります。

16. アカウントのアクティブ化コードを入力し、**[Next]**（次へ）をクリックします。

17. 確認ダイアログ ボックスが表示されたら、**[OK]**をクリックします。

既存のオンライン復元アカウントの管理

オンライン復元アカウントを作成すると、SafeBoot の[Recovery Service]の Web サイトにアクセスできるようになります。このサイトでは、パスワードをなくしたときのコンピュータへのアクセスの復元、個人設定の変更、オンライン復元アカウントで使用するパスワードの再設定、およびアカウントの表示または更新を行うことができます。

1. Drive Encryption を開き、**[Recovery]**（復元）をクリックします。

2. **[Manage]**（管理）をクリックします。

3. SafeBoot の[Recovery Service]の Web ページが表示されたら、**[Recovery Service Account]**（復元サービス アカウント）または**[Recovery Process]**（復旧手順）をクリックします。

4. 復元サービス ログオン ページに、ユーザの電子メール アドレス、パスワード、およびボックスに表示されている数字と文字を入力します。

5. **[Logon]**（ログオン）をクリックします。

6. **[Profile]**（プロファイル）をクリックして、電話番号や課金先の住所などの個人情報を更新します。

   または

   [Reset Password]（パスワードの再設定）をクリックし、パスワードを再設定または変更します。

   または

   [My Subscriptions]（マイ サブスクリプション）をクリックし、現在のサブスクリプション情報を表示します。

注記： [My Subscriptions]ページでは、ユーザのサブスクリプションを更新することもできます。更新するには、**[Renew Subscription]**（サブスクリプションの更新）をクリックします。

復元の実行

ローカル復元の実行

1. コンピュータの電源を入れます。

2. バックアップ キーを保管しているリムーバブル ストレージ デバイスを装着します。

3. Drive Encryption for HP ProtectTools のログオン ダイアログ ボックスが表示されたら、**[Cancel]**（キャンセル）をクリックします。

4. 画面の左下隅にある**[Option]**（オプション）をクリックしてから、**[Recovery]**（復元）をクリックします。

5. **[Local recovery]**（ローカル復元）をクリックしてから、**[Next]**（次へ）をクリックします。

6. バックアップ キーが含まれているファイルを選択するか、**[Browse]**（参照）をクリックして該当のファイルを探してから、**[Next]**（次へ）をクリックします。

7. 確認ダイアログ ボックスが表示されたら、**[OK]**をクリックします。

   復元プロセスが完了して、コンピュータが起動します。

注記： 復元の実行後は、パスワードを再設定することを強くおすすめします。

オンライン復元の実行

注記： ここでは、インターネットに接続している別のコンピュータを使用したオンライン復元の方法について説明します。このようなコンピュータを使用できない場合は、HP のサポート窓口にお問い合わせください。

1. コンピュータの電源を入れます。

2. Drive Encryption for HP ProtectTools のログオン ダイアログ ボックスが表示されたら、**[Cancel]**をクリックします。

3. 画面の左下隅にある**[Option]**をクリックしてから、**[Recovery]**をクリックします。

4. **[Web recovery]**（Web 復元）をクリックし、**[Next]**（次へ）をクリックします。

5. クライアント コードを記録し、**[Next]**（次へ）をクリックします。

6. インターネットに接続している別のコンピュータで、SafeBoot の[Recovery Service]の Web サイト、http://www.safeboot-hp.com/（英語サイト）にアクセスします。

7. **[Recovery Process]**（復旧手順）をクリックします。

8. 復元サービス ログオン ページに、ユーザの電子メール アドレス、パスワード、およびボックスに表示されている数字と文字を入力します。

9. **[Logon]**（ログオン）をクリックします。

10. **[Recovery Process]**をクリックします。

11. 復元中のコンピュータから記録したクライアント コードを入力し、ボックスに表示されている数字と文字を入力します。

12. **[Submit]**（送信）をクリックします。

13. 応答キーの各行を記録します。

14. 復元中のコンピュータに、SafeBoot の[Recovery Service]の Web サイトで記録した応答キーの行 1 を入力し、**[Enter]**（入力）をクリックします。

15. 応答キーの行 2 を入力し、**[Enter]**をクリックします。

16. 応答キーの行 3 を入力し、**[Enter]**をクリックします。

17. 応答キーの行 4 を入力し、**[Enter]**をクリックします。

    注記： 応答キーの行 4 は、最初の 3 行よりも短くなります。

18. **[Finish]**（完了）をクリックします。

注記： 復元の実行後は、パスワードを再設定することを強くおすすめします。

4 Privacy Manager for HP ProtectTools（一部のモデルのみ）

Privacy Manager for HP ProtectTools を使用すると、電子メール、Microsoft® Office ドキュメント、またはインスタント メッセージ（IM）を使用するときに、高度なセキュリティ ログオン（認証）方法を使用して、通信の発信元、整合性、セキュリティを確認できます。

Privacy Manager では、HP ProtectTools Security Manager（セキュリティ マネージャ）が提供するセキュリティ インフラストラクチャを活用します。HP ProtectTools セキュリティ マネージャのセキュリティ ログオン方法は、以下のとおりです。

- 指紋認証
- Windows®のパスワード
- HP ProtectTools Java™ Card

Privacy Manager では、上記のセキュリティ ログオン方法を使用できます。

Privacy Manager の起動

Privacy Manager を起動するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。
2. **[Privacy Manager: Sign and Chat]**（Privacy Manager:署名とチャット）をクリックします。

または

タスクバーの右端の通知領域にある**[HP ProtectTools]**アイコンを右クリックしてから**[Privacy Manager: Sign and Chat]→[Configuration]**（構成）の順にクリックします。

または

[Microsoft Outlook]の電子メール メッセージのツールバーで**[Send Securely]**（安全に送信）の横にある下向きの矢印をクリックしてから、**[Certificate Manager]**（証明書マネージャ）または**[Trusted Contact Manager]**（信頼済み連絡先マネージャ）をクリックします。

または

Microsoft Office ドキュメントのツールバーで**[Sign and Encrypt]**（署名と暗号化）の横にある下向きの矢印をクリックしてから、**[Certificate Manager]**（証明書マネージャ）または**[Trusted Contact Manager]**（信頼済み連絡先マネージャ）をクリックします。

セットアップ手順

Privacy Manager Certificate の管理

Manager Certificate は、公開キー基盤（PKI）と呼ばれる暗号化技術を使用して、データとメッセージを保護します。PKI の利用にあたり、ユーザは暗号キーと、証明機関（CA）が発行する Privacy Manager Certificate を取得する必要があります。認証を定期的に要求するだけのほとんどのデータ暗号化ソフトウェアや認証ソフトウェアとは異なり、Privacy Manager は、暗号キーを使用して電子メール メッセージや Microsoft Office ドキュメントに署名するたびに認証を要求します。Privacy Manager によって、重要な情報の保存と送信の処理が安全で確実なものとなります。

Privacy Manager Certificate の要求とインストール

Privacy Manager の機能を使用するには、有効な電子メール アドレスを使用して Privacy Manager から Privacy Manager Certificate を要求し、インストールしておく必要があります。この電子メール アドレスは、Privacy Manager Certificate を要求するコンピュータの[Microsoft Outlook]のアカウントとして設定する必要があります。

Privacy Manager Certificate の要求

1. Privacy Manager を開き、**[Certificate Manager]**（証明書マネージャ）をクリックします。
2. **[Request a Privacy Manager Certificate]**（Privacy Manager Certificate の要求）をクリックします。
3. [Welcome]（ようこそ）ページで、画面に表示される内容を確認してから**[Next]**（次へ）をクリックします。
4. [License Agreement]（使用許諾契約）ページで、使用許諾契約の内容を確認します。
5. **[Check here to accept the terms of this license agreement]**（使用許諾契約の条件に同意する場合はチェック）の隣のチェック ボックスにチェックが入っていることを確認してから、**[Next]**（次へ）をクリックします。
6. [Your Certificate Details]（証明書の詳細）ページで、求められた情報を入力してから**[Next]**（次へ）をクリックします。
7. [Certificate Request Accepted]（証明書の要求が承認されました）ページで、**[Finish]**（完了）をクリックします。

   [Microsoft Outlook]に、Privacy Manager Certificate が添付された電子メールが届きます。

Privacy Manager Certificate のインストール

1. Privacy Manager Certificate の添付された電子メールを受信したら、メールを開き、メッセージの右下隅にある**[Setup]**（設定）ボタンをクリックします。
2. 選択したセキュリティ ログオン方法で認証します。
3. [Certificate Installed]（証明書がインストールされました）ページで、**[Next]**（次へ）をクリックします。
4. [Certificate Backup]（証明書のバックアップ）ページで、バックアップ ファイルの保存先と名前を入力するか、または**[Browse]**（参照）をクリックして保存先を探します。

△ **注意：** ファイルはハードドライブ以外の場所に保存し、安全な場所に保管してください。本人以外はこのファイルを使用できません。また、Privacy Manager Certificate と、関連するキーを復元しなければならない場合には、このファイルが必要です。

5. パスワードの入力と確認を行い、**[Next]**（次へ）をクリックします。
6. 選択したセキュリティ ログオン方法で認証します。
7. Trusted Contact の招待の処理を始める場合は、画面の説明に沿って操作します。

   または

   [Cancel]（キャンセル）をクリックすると、後で Trusted Contact を追加できます。詳しくは、「Trusted Contact の管理」を参照してください。

Privacy Manager Certificate の詳細の表示

1. Privacy Manager を開き、**[Certificate Manager]**（証明書マネージャ）をクリックします。
2. Privacy Manager Certificate をクリックします。
3. **[Certificate details]**（証明書の詳細）をクリックします。
4. 詳細の確認を終えたら、**[OK]**をクリックします。

Privacy Manager Certificate の更新

Privacy Manager Certificate が有効期限に近づくと、更新が必要であることが通知されます。

1. Privacy Manager を開き、**[Certificate Manager]**（証明書マネージャ）をクリックします。
2. Privacy Manager Certificate をクリックします。
3. **[Renew certificate]**（証明書の更新）をクリックします。
4. 画面の説明に沿って操作し、新しい Privacy Manager Certificate を購入します。

注記： Privacy Manager Certificate の更新処理を行っても、古い Privacy Manager Certificate は置き換えられません。新しい Privacy Manager Certificate を購入したら、「Privacy Manager Certificate の要求とインストール」に記載されている手順でインストールする必要があります。

Privacy Manager Certificate の初期設定の指定

お使いのコンピュータに別の証明機関からの証明書がインストールされている場合でも、Privacy Manager には Privacy Manager Certificate のみが表示されます。

コンピュータに Privacy Manager からインストールした Privacy Manager Certificate が複数ある場合は、どれか 1 つを初期設定の証明書として指定できます。

1. Privacy Manager を開き、**[Certificate Manager]**（証明書マネージャ）をクリックします。
2. 初期設定として使用する Privacy Manager Certificate をクリックしてから、**[Set default]**（初期値の指定）をクリックします。
3. **[OK]**をクリックします。

注記： 初期設定の Privacy Manager Certificate をいつも使用する必要はありません。Privacy Manager のさまざまな機能によって、使用する Privacy Manager Certificate を選択できます。

Privacy Manager Certificate の削除

Privacy Manager Certificate を削除すると、この証明書で暗号化したファイルを開いたり、データを表示することができなくなります。間違えて Privacy Manager Certificate を削除した場合は、証明書のインストール時に作成したバックアップ ファイルを使用して証明書を復元できます。

Privacy Manager Certificate を削除するには、以下の手順で操作します。

1. Privacy Manager を開き、**[Certificate Manager]**（証明書マネージャ）をクリックします。
2. 削除する Privacy Manager Certificate をクリックしてから、**[Advanced]**（詳細）をクリックします。
3. **[Delete]**（削除）をクリックします。
4. 確認用のダイアログ ボックスが表示されたら、**[Yes]**（はい）をクリックします。
5. **[Close]**（閉じる）をクリックし、**[Apply]**（適用）をクリックします。

Privacy Manager Certificate の復元

間違えて Privacy Manager Certificate を削除した場合は、証明書のインストールまたはエクスポートの際に作成したバックアップ ファイルを使用して証明書を復元できます。

1. Privacy Manager を開き、**[Migration]**（移行）をクリックします。
2. **[Import migration file]**（移行ファイルのインポート）をクリックします。
3. [Migration File]（移行ファイル）ページをクリックして、**[Browse]**（参照）をクリックし、Privacy Manager Certificate のインストールまたはエクスポートの際に作成した.dppsm ファイルを探してから、**[Next]**（次へ）をクリックします。
4. [Migration File Imported]（移行ファイルをインポートしました）ページで、**[Finish]**（完了）をクリックします。
5. **[Close]**（閉じる）をクリックし、**[Apply]**（適用）をクリックします。

注記： 詳しくは、「Privacy Manager Certificate のインストール」または「Privacy Manager Certificate と Trusted Contact のエクスポート」を参照してください。

Privacy Manager Certificate の廃止

お使いの Privacy Manager Certificate のセキュリティに問題があると感じる場合、その証明書を廃止できます。

注記： Privacy Manager Certificate を廃止しても、削除はされません。この証明書は、暗号化したファイルを表示するために引き続き使用できます。

1. Privacy Manager を開き、**[Certificate Manager]**（証明書マネージャ）をクリックします。
2. **[Advanced]**（詳細）をクリックします。
3. 廃止する Privacy Manager Certificate をクリックしてから、**[Revoke]**（廃止）をクリックします。
4. 確認用のダイアログ ボックスが表示されたら、**[Yes]**（はい）をクリックします。

5. 選択したセキュリティ ログオン方法で認証します。

6. 画面に表示される説明に沿って操作します。

Trusted Contact の管理

Trusted Contact とは、安全に通信が出来るように、互いに Privacy Manager Certificate を交換したユーザのことです。

Trusted Contact の追加

1. Trusted Contact の受信者に、電子メールで招待状を送信します。

2. Trusted Contact の受信者が、この電子メールに返信します。

3. Trusted Contact の受信者から返信メールを受け取ったら、[Accept]（承認）をクリックします。

Trusted Contact の電子メール招待状は、個々の受信者宛てに送信することも、[Microsoft Outlook]のアドレス帳に記載されているすべての連絡先に送信することもできます。

注記： Trusted Contact になるための招待状に返信するには、Trusted Contact の受信者のコンピュータに、Privacy Manager または別のクライアントがインストールされている必要があります。別のクライアントのインストールについて詳しくは、DigitalPersona の Web サイト http://DigitalPersona.com/PrivacyManager（英語サイト）にアクセスしてください。

Trusted Contact の追加

1. Privacy Manager を開き、**[Trusted Contacts Manager]**（信頼済み連絡先マネージャ）→**[Invite Contacts]**（連絡先の招待）の順にクリックします。

   または

   [Microsoft Outlook]で、ツールバーの**[Send Securely]**（安全に送信）の横にある下向きの矢印をクリックしてから、**[Invite Contacts]**をクリックします。

2. [Select Certificate]（証明書の選択）ダイアログ ボックスが表示された場合は、使用する Privacy Manager Certificate をクリックしてから**[OK]**をクリックします。

3. [Trusted Contact Invitation]（信頼済み連絡先の招待）ダイアログ ボックスが表示されたら、画面に表示されている内容を確認してから**[OK]**をクリックします。

   自動的に電子メールが生成されます。

4. Trusted Contact に追加する受信者の電子メール アドレスを、1 つ以上入力します。

5. テキストを編集し、自分の名前を署名します（オプション）。

6. **[Send]**（送信）をクリックします。

   注記： Privacy Manager Certificate を取得していない場合、Trusted Contact 要求の送信には Privacy Manager Certificate が必要というメッセージが表示されます。[OK]をクリックして、[Certificate Request Wizard]（証明書の要求ウィザード）を起動します。

7. 選択したセキュリティ ログオン方法で認証します。

8. Trusted Contact になるための招待を承認した返信メールを受信者から受け取ったら、電子メール右下隅の[Accept]（承認）をクリックします。

ダイアログ ボックスが開き、受信者が Trusted Contact の一覧に正常に追加されたことを確認できます。

9. **[OK]**をクリックします。

[Microsoft Outlook]のアドレス帳を使用した Trusted Contact の追加

1. Privacy Manager を開き、**[Trusted Contacts Manager]**（信頼済み連絡先マネージャ）→**[Invite Contacts]**（連絡先の招待）の順にクリックします。

   または

   [Microsoft Outlook]で、ツールバーの**[Send Securely]**（安全に送信）の横にある下向きの矢印をクリックしてから、**[Invite All My Outlook Contacts]**（Outlook のすべての連絡先を招待）をクリックします。

2. [Trusted Contact Invitation]（信頼済み連絡先の招待）ページが開いたら、Trusted Contact に追加する受信者の電子メール アドレスを選択してから**[Next]**（次へ）をクリックします。

3. [Sending Invitation]（招待状の送信）ページが開いたら、**[Finish]**（完了）をクリックします。

   選択した[Microsoft Outlook]の電子メール アドレスを一覧表示した電子メールが自動生成されます。

4. テキストを編集し、自分の名前を署名します（オプション）。

5. **[Send]**（送信）をクリックします。

   注記： Privacy Manager Certificate を取得していない場合、Trusted Contact 要求の送信には Privacy Manager Certificate が必要というメッセージが表示されます。**[OK]**をクリックして、[Certificate Request Wizard]（証明書の要求ウィザード）を起動します。

6. 選択したセキュリティ ログオン方法で認証します。

   注記： Trusted Contact の受信者は、電子メールを受信すると、電子メールを開いて右下隅の[Accept]（承認）をクリックし、確認用のダイアログ ボックスが表示されたら[OK]をクリックする必要があります。

7. Trusted Contact になるための招待を承認した返信メールを受信者から受け取ったら、電子メール右下隅の[Accept]をクリックします。

   ダイアログ ボックスが開き、受信者が Trusted Contact の一覧に正常に追加されたことを確認できます。

8. **[OK]**をクリックします。

Trusted Contact の詳細の表示

1. Privacy Manager を開き、**[Trusted Contacts Manager]**（信頼済み連絡先マネージャ）をクリックします。

2. Trusted Contact をクリックします。

3. **[Contact details]**（連絡先の詳細）をクリックします。

4. 詳細の確認を終えたら、**[OK]**をクリックします。

Trusted Contact の削除

1. Privacy Manager を開き、**[Trusted Contacts Manager]**（信頼済み連絡先マネージャ）をクリックします。
2. 削除する Trusted Contact をクリックします。
3. **[Delete contact]**（連絡先の削除）をクリックします。
4. 確認用のダイアログ ボックスが表示されたら、**[Yes]**（はい）をクリックします。

Trusted Contact の廃止状態の確認

1. Privacy Manager を開き、**[Trusted Contacts Manager]**（信頼済み連絡先マネージャ）をクリックします。
2. Trusted Contact をクリックします。
3. **[Advanced]**（詳細）ボタンをクリックします。

   [Advanced Trusted Contact Management]（高度な Trusted Contact 管理）ダイアログ ボックスが開きます。
4. **[Check Revocation]**（廃止の確認）をクリックします。
5. **[Close]**（閉じる）をクリックします。

一般的なタスク

Microsoft Office ドキュメントでの Privacy Manager の使用

Privacy Manager Certificate をインストールすると、[Microsoft Word]、[Microsoft Excel]、および[Microsoft PowerPoint]のすべてのドキュメントのツールバーの右側に、[Sign and Encrypt]（署名と暗号化）ボタンが表示されます。

Microsoft Office ドキュメントでの Privacy Manager の設定

1. Privacy Manager を開き、**[Settings]**（設定）をクリックしてから**[Documents]**（ドキュメント）タブをクリックします。

   または

   Microsoft Office ドキュメントのツールバーで、**[Sign and Encrypt]**の横にある下向きの矢印をクリックしてから**[Settings]**をクリックします。

2. 設定する操作を選択し、**[OK]**をクリックします。

Microsoft Office ドキュメントへの署名

1. [Microsoft Word]、[Microsoft Excel]、または[Microsoft PowerPoint]でドキュメントを作成し、保存します。
2. **[Sign and Encrypt]**の横にある下向きの矢印をクリックしてから、**[Sign Document]**（ドキュメントへの署名）をクリックします。
3. 選択したセキュリティ ログオン方法で認証します。
4. 確認用のダイアログ ボックスが表示されたら、画面に表示されている内容を確認してから**[OK]**をクリックします。

後でドキュメントを編集する場合は、以下の手順で操作します。

1. 画面の左上隅にある**[Office]**ボタンをクリックします。
2. **[Prepare]**（準備）→**[Mark as Final]**（最終版としてマーク）の順にクリックします。
3. 確認用のダイアログ ボックスが表示されたら、**[Yes]**（はい）をクリックして作業を続けます。
4. 編集が終わったら、再びドキュメントに署名します。

[Microsoft Word]または[Microsoft Excel]ドキュメント署名時の署名欄の追加

Privacy Manager では、[Microsoft Word]または[Microsoft Excel]ドキュメントに署名する際に署名欄を追加できます。

1. [Microsoft Word]または[Microsoft Excel]でドキュメントを作成し、保存します。
2. **[Home]**（ホーム）メニューをクリックします。
3. **[Sign and Encrypt]**（署名と暗号化）の横にある下向きの矢印をクリックしてから、**[Add Signature Line Before Signing]**（署名の前に署名欄を追加）をクリックします。

> 注記： このオプションを選択すると、[Add Signature Line Before Signing]の横にチェック マークが表示されます。初期設定では、このオプションは有効になっています。

4. **[Sign and Encrypt]**の横にある下向きの矢印をクリックしてから、**[Sign Document]**（ドキュメントへの署名）をクリックします。

5. 選択したセキュリティ ログオン方法で認証します。

[Microsoft Word]または[Microsoft Excel]ドキュメントに、推奨する署名者を追加する

推奨する署名者を指名することによって、ドキュメントに複数の署名欄を追加できます。推奨する署名者とは、ドキュメントに署名欄を追加するために[Microsoft Word]または[Microsoft Excel]ドキュメントの所有者が指名したユーザのことです。推奨する署名者には自分自身を指名することも、別の人物を指名してドキュメントへの署名を依頼することもできます。たとえば、部署内の全員の署名が必要なドキュメントを準備する場合、特定の日付で署名するよう指示した全員分の署名欄を、ドキュメントの最終ページの最下部に設けることができます。

[Microsoft Word]または[Microsoft Excel]ドキュメントに、推奨する署名者を追加するには、以下の手順で操作します。

1. [Microsoft Word]または[Microsoft Excel]でドキュメントを作成し、保存します。

2. **[挿入]**メニューをクリックします。

3. ツールバーの**[Text]**（テキスト）グループで、**[Signature Line]**（署名欄）の横にある矢印をクリックしてから**[Privacy Manager Signature Provider]**（Privacy Manager 署名プロバイダ）をクリックします。

   [Signature Setup]（署名の設定）ダイアログ ボックスが表示されます。

4. ボックス内の**[Suggested signer]**（推奨する署名者）の下に、推奨する署名者の名前を入力します。

5. ボックス内の**[Instructions to the signer]**（署名者への指示）の下に、この推奨する署名者へのメッセージを入力します。

   注記： このメッセージはタイトルとして表示されますが、ドキュメントに署名すると、削除したりユーザのタイトルに置き換えたりすることができます。

6. **[Show sign date in signature line]**（署名欄に署名日を表示）チェック ボックスにチェックを入れて、日付を表示します。

7. **[Show signer's title in signature line]**（署名欄に署名者のタイトルを表示）チェック ボックスにチェックを入れて、タイトルを表示します。

   注記： ドキュメントの所有者が、推奨する署名者を自身のドキュメントに割り当てているので、**[Show sign date in signature line]**および**[Show signer's title in signature line]**の各チェック ボックスにチェックが入っていないと、推奨する署名者は署名欄に日付やタイトルを表示できません。これには推奨する署名者によるドキュメント設定は関係しません。

8. **[OK]**をクリックします。

推奨する署名者の署名欄の追加

推奨する署名者がドキュメントを開くと、自分の名前が角かっこで囲まれて表示され、署名を求められていることがわかります。

ドキュメントに署名するには、以下の手順で操作します。

1. 適切な署名欄をダブルクリックします。

2. 選択したセキュリティ ログオン方法で認証します。

ドキュメントの所有者が指定した設定に従って、署名欄が表示されます。

Microsoft Office ドキュメントの暗号化

自分自身と Trusted Contact のために、Microsoft Office ドキュメントを暗号化できます。ドキュメントを暗号化してから閉じると、自分自身と一覧から選択した Trusted Contact は、このドキュメントを開く際に認証が必要となります。

Microsoft Office ドキュメントを暗号化するには、以下の手順で操作します。

1. [Microsoft Word]、[Microsoft Excel]、または[Microsoft PowerPoint]でドキュメントを作成し、保存します。
2. **[Home]**（ホーム）メニューをクリックします。
3. **[Sign and Encrypt]**（署名と暗号化）の横にある下向きの矢印をクリックしてから、**[Encrypt Document]**（ドキュメントの暗号化）をクリックします。

   [Select Trusted Contacts]（信頼済み連絡先の選択）ダイアログ ボックスが表示されます。
4. ドキュメントを開いて内容を閲覧できるようにする Trusted Contact の名前をクリックします。

   注記： Trusted Contact の名前を複数選択するには、ctrl キーを押しながら個々の名前をクリックします。
5. **[OK]**をクリックします。
6. 選択したセキュリティ ログオン方法で認証します。

後でドキュメントを編集する場合は、「Microsoft Office ドキュメントへの署名」に記載されている手順で操作します。暗号化を解除すると、ドキュメントを編集できます。再びドキュメントを暗号化するには、ここに記載されている手順で操作します。

Microsoft Office ドキュメントの暗号化の解除

Microsoft Office ドキュメントの暗号化を解除すると、自分自身と Trusted Contact は、認証なしでこのドキュメントを開いて内容を閲覧できるようになります。

Microsoft Office ドキュメントの暗号化を解除するには、以下の手順で操作します。

1. 暗号化された[Microsoft Word]、[Microsoft Excel]、または[Microsoft PowerPoint]ドキュメントを開きます。
2. 選択したセキュリティ ログオン方法で認証します。
3. **[Home]**（ホーム）メニューをクリックします。
4. **[Sign and Encrypt]**（署名と暗号化）の横にある下向きの矢印をクリックしてから、**[Remove Encryption]**（暗号化の解除）をクリックします。

暗号化された Microsoft Office ドキュメントの送信

電子メール メッセージに、暗号化された Microsoft Office ドキュメントを添付できます。電子メール自体への署名や暗号化は不要です。これには、ファイルを添付した一般の電子メールの場合と同様に、署名または暗号化したドキュメントを添付した電子メールを作成し、送信します。

ただし、最適なセキュリティのため、署名または暗号化された Microsoft Office ドキュメントを添付する際に電子メールを暗号化することをおすすめします。

署名および暗号化した Microsoft Office ドキュメントを添付して、封印した電子メールを送信するには、以下の手順で操作します。

1. [Microsoft Outlook]で、**[新規作成]**または**[返信]**をクリックします。
2. 電子メール メッセージを入力します。
3. Microsoft Office ドキュメントを添付します。
4. 詳しい手順については、「電子メール メッセージの封印および送信」を参照してください。

署名付き Microsoft Office ドキュメントの表示

注記： 署名付き Microsoft Office ドキュメントを表示するには、Privacy Manager Certificate は不要です。

署名付き Microsoft Office ドキュメントを開くと、ドキュメントの横に[Signatures]（署名）ダイアログ ボックスが開き、ドキュメントに署名したユーザの名前と署名日が表示されます。名前を右クリックすると、詳細を確認できます。

暗号化された Microsoft Office ドキュメントの表示

暗号化された Microsoft Office ドキュメントを別のコンピュータから閲覧するには、そのコンピュータに Privacy Manager をインストールしておく必要があります。また、ファイルの暗号化に使用した Privacy Manager Certificate をインポートする必要があります。

Trusted Contact が暗号化された Microsoft Office ドキュメントを閲覧するには、Privacy Manager Certificate が必要です。なお、コンピュータに Privacy Manager をインストールしておく必要があります。また、暗号化された Microsoft Office ドキュメントの所有者が、この Trusted Contact を選択している必要があります。

[Microsoft Outlook]での Privacy Manager の使用

Privacy Manager をインストールすると、[Microsoft Outlook]のツールバーに[Privacy]（プライバシ）ボタンが表示されるようになります。また、[Microsoft Outlook]の各電子メール メッセージのツールバーに[Send Securely]（安全に送信）ボタンが表示されるようになります。

[Microsoft Outlook]用の Privacy Manager の設定

1. **[Privacy Manager]**を開き、**[Settings]**（設定）をクリックしてから**[E-mail]**（電子メール）タブをクリックします。

   または

   [Microsoft Outlook]のメインのツールバーで、**[Privacy]**の横にある下向きの矢印をクリックしてから**[Settings]**をクリックします。

   または

   Microsoft の電子メール メッセージのツールバーで、**[Send Securely]**の横にある下向きの矢印をクリックしてから**[Settings]**をクリックします。

2. 安全な電子メールを送信する際に実行する操作を選択し、**[OK]**をクリックします。

電子メール メッセージの署名および送信

▲ [Microsoft Outlook]で、**[新規作成]**または**[返信]**をクリックします。

▲ 電子メール メッセージを入力します。

▲ **[Send Securely]**の横にある下向きの矢印をクリックしてから、**[Sign and Send]**（署名して送信）をクリックします。

▲ 選択したセキュリティ ログオン方法で認証します。

電子メール メッセージの封印および送信

デジタル処理によって署名、封印（暗号化）されている、封印された電子メールを閲覧できるのは、Trusted Contacts の一覧から選択したユーザのみです。

電子メールを封印して Trusted Contact に送信するには、以下の手順で操作します。

1. [Microsoft Outlook]で、**[新規作成]**または**[返信]**をクリックします。
2. 電子メール メッセージを入力します。
3. **[Send Securely]**の横にある下向きの矢印をクリックしてから、**[Seal for Trusted Contacts and Send]**（信頼済み連絡先宛てに封印して送信）をクリックします。
4. 選択したセキュリティ ログオン方法で認証します。

封印された電子メール メッセージの表示

封印された電子メール メッセージを開くと、電子メールの見出しにセキュリティ ラベルが表示されます。このセキュリティ ラベルには、以下の情報が記載されています。

- 電子メールに署名した人物の身元確認に使用された証明書
- 電子メールに署名した人物の証明書の確認に使用された製品

[Windows Live Messenger]での Privacy Manager の使用

Privacy Manager Chat 機能の追加

[Windows Live Messenger]に Privacy Manager Chat 機能を追加するには、以下の手順で操作します。

1. [Windows Live Home]（Windows Live ホーム）にログインします。
2. **[Windows Live]**アイコンをクリックしてから**[Windows Live Services]**（Windows Live サービス）をクリックします。
3. **[Gallery]**（ギャラリ）→**[Messenger]**（メッセンジャ）の順にクリックします。
4. **[Activities]**（操作）→**[Safety and Security]**（安全とセキュリティ）の順にクリックします。
5. **[Privacy Manager Chat]**をクリックし、画面の説明に沿って操作します。

Privacy Manager Chat の開始

注記： Privacy Manager Chat を使用するには、双方に Privacy Manager と Privacy Manager Certificate がインストールされている必要があります。Privacy Manager Certificate のインストールについて詳しくは、5 ページの「Privacy Manager Certificate の要求とインストール」を参照してください。

1. [Windows Live Messenger]で Privacy Manager Chat を始めるには、以下のどれかの手順で操作します。

   a. [Live Messenger]でオンライン上の連絡相手を右クリックしてから、**[Start an Activity]**（操作の開始）を選択します。

   b. **[Start Privacy Manager Chat]**（Privacy Manager Chat の開始）をクリックします。

   または

   a. [Live Messenger]でオンライン上の連絡相手をダブルクリックしてから、**[Conversation]**（会話）メニューをクリックします。

   b. **[Action]**（アクション）→**[Start Privacy Manager Chat]**の順にクリックします。

   Privacy Manager Chat を始める際には、Privacy Manager から連絡相手に招待状が送信されます。招待された相手が承認すると、[Privacy Manager Chat]ウィンドウが開きます。招待された相手が Privacy Manager を持っていない場合は、ダウンロードするよう要求されます。

2. **[Start]**（開始）をクリックすると、安全なチャットが始まります。

[Windows Live Messenger]用の Privacy Manager Chat の設定

1. Privacy Manager Chat で、**[Settings]**（設定）ボタンをクリックします。

   または

   Privacy Manager で、**[Settings]**（設定）をクリックしてから**[Chat]**（チャット）タブをクリックします。

   または

   Privacy Manager History Viewer で、**[Settings]**（設定）ボタンをクリックします。

2. セッションをロックするまでの Privacy Manager Chat の待機時間を指定するには、**[Lock session after _ minutes of inactivity]**（操作しない状態が_分の経過でセッションをロック）ボックスで数を選択します。

3. チャット セッションの履歴フォルダを指定するには、**[Browse]**（参照）をクリックしてフォルダを探してから、**[OK]**をクリックします。

4. セッションを閉じる際に自動的にセッションを暗号化して保存するには、**[Automatically save secure chat history]**（安全なチャット履歴を自動的に保存）チェック ボックスにチェックを入れます。

5. **[OK]**をクリックします。

[Privacy Manager Chat]ウィンドウでのチャット

Privacy Manager Chat を開始すると、[Windows Live Messenger]に[Privacy Manager Chat]ウィンドウが開きます。Privacy Manager Chat の使い方は、一般的な[Windows Live Messenger]の使い方と同様です。ただし、以下の機能は[Privacy Manager Chat]ウィンドウでのみ利用できます。

- **Save**（保存）：このボタンをクリックすると、設定時に指定したフォルダにチャット セッションが保存されます。セッションを閉じるたびに自動的に保存するよう Privacy Manager Chat を設定することもできます。
- **Hide all**（すべて非表示）と **Show all**（すべて表示）：各ボタンをクリックすると、[Secure Communications]（セキュア通信）ウィンドウに表示されているメッセージが展開されたり折りたたまれたりします。メッセージのヘッダをクリックして、個々のメッセージの非表示と表示を切り替えることもできます。
- **Are you there?**（相手確認）：このボタンをクリックすると、相手からの認証が要求されます。
- **Lock**（ロック）：このボタンをクリックすると、[Privacy Manager Chat]ウィンドウが閉じて[Chat Entry]（チャットの登録）ウィンドウに戻ります。再び[Secure Communications]ウィンドウを表示するには、**[Resume the session]**（セッションの再開）をクリックし、選択したセキュリティ ログオン方法で認証します。
- **Send**（送信）：このボタンをクリックすると、暗号化されたメッセージが相手に送信されます。
- **Send signed**（署名して送信）：このチェック ボックスにチェックを入れると、メッセージに電子署名が付加され、メッセージが暗号化されます。メッセージが改ざんされると、受信者がメッセージを受け取った際に、無効なメッセージとしてマークされます。署名付きメッセージを送信するたびに認証が必要です。
- **Send hidden**（非表示で送信）：このチェック ボックスにチェックを入れるとメッセージが暗号化され、メッセージの見出しのみを表示して送信されます。相手がメッセージの内容を読むには、認証する必要があります。

チャット履歴の表示

Privacy Manager Chat History Viewer には、暗号化された Privacy Manager Chat セッション ファイルが表示されます。セッションは、[Privacy Manager Chat]ウィンドウの[Save]（保存）をクリックするか、Privacy Manager の[Chat]（チャット）タブで自動保存を設定することによって保存されます。このビューアには、セッションごとに、（暗号化された）連絡先のスクリーン名と、セッションの開始日時と終了日時が表示されます。初期設定では、設定したすべての電子メール アカウントのセッションが表示されます。**[Display history for]**（履歴を表示）メニューを使用すると、特定のアカウントのみを選択して表示できます。

Chat History Viewer の起動

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。
2. **[Privacy Manager: Sign and Chat]**（Privacy Manager:署名とチャット）→**[Chat History Viewer]**の順にクリックします。

   または

   ▲ チャット セッションで、**[History Viewer]**（履歴ビューア）または**[History]**（履歴）をクリックします。

   または

   ▲ [Chat Configuration]（チャットの設定）ページで、**[Start Live Messenger History Viewer]**（Live Messenger 履歴ビューアの起動）をクリックします。

すべてのセッションの公開

すべてのセッションを公開すると、選択中のセッション（複数可）と、同一アカウントのすべてのセッションについて、暗号化された Contact Screen Name が表示されます。

1. Chat History Viewer で、任意のセッションを右クリックしてから**[Reveal All Sessions]**（すべてのセッションの公開）を選択します。
2. 選択したセキュリティ ログオン方法で認証します。

   Contact Screen Name の暗号化が解除されます。
3. 任意のセッションをダブルクリックして、内容を表示します。

特定のアカウントのセッションの公開

セッションを公開すると、選択中のセッションの暗号化された Contact Screen Name が表示されます。

1. Chat History Viewer で、任意のセッションを右クリックしてから**[Reveal Session]**（セッションの公開）を選択します。
2. 選択したセキュリティ ログオン方法で認証します。

   Contact Screen Name の暗号化が解除されます。
3. 公開されたセッションをダブルクリックして、内容を表示します。

注記： 同じ証明書で暗号化された別のセッションは、開錠されたアイコンで表示されます。これらのセッションは、認証しないでダブルクリックするだけで表示できます。別の証明書で暗号化されたセッションは、施錠されたアイコンで表示されます。これらのセッションの Contact Screen Name や内容を表示するには、別途認証が必要です。

セッション ID の表示

▲ Chat History Viewer で、任意の公開されたセッションを右クリックしてから**[View session ID]**（セッション ID の表示）を選択します。

セッションの表示

セッションを表示すると、表示用のファイルが開きます。セッションが公開されていなかった場合は（暗号化された Contact Screen Name が表示されます）、ここで公開されます。

1. Chat History Viewer で、任意の公開されたセッションを右クリックして**[View]**（表示）を選択します。
2. 画面に指示が表示されたら、選択したセキュリティ ログオン方法で認証します。

   セッションの内容の暗号化が解除されます。

テキストの指定によるセッションの検索

ビューアのウィンドウに表示されている、公開された（暗号化が解除された）セッションのテキストのみ検索ができます。これらのセッションでは、Contact Screen Name が平文で表示されています。

1. Chat History Viewer で、**[Search]**（検索）ボタンをクリックします。
2. 検索するテキストを入力し、検索パラメータを設定してから**[OK]**をクリックします。

   テキストを含むセッションが、ビューアのウィンドウに強調表示されます。

セッションの削除

1. チャット履歴セッションを選択します。
2. **[Delete]**（削除）をクリックします。

列の追加または削除

初期設定では、Chat History Viewer に、最もよく使用する列が 3 つ表示されます。列は画面に追加したり、画面から削除したりすることができます。

画面に列を追加するには、以下の手順で操作します。

1. 任意の列見出しを右クリックしてから、**[Add/Remove Columns]**（列の追加/削除）を選択します。
2. 左側のパネルの列見出しを選択してから**[Add]**（追加）をクリックして、列を右側のパネルに移動します。

画面から列を削除するには、以下の手順で操作します。

1. 任意の列見出しを右クリックしてから、**[Add/Remove Columns]**を選択します。
2. 右側のパネルの列見出しを選択してから**[Remove]**をクリックして、列を左側のパネルに移動します。

表示中のセッションのフィルタリング

Chat History Viewer には、すべてのアカウントのセッションが一覧表示されます。

特定のアカウントのセッションの表示

▲ Chat History Viewer で、**[Display history for]**（履歴を表示）メニューからアカウントを選択します。

日付範囲内のセッションの表示

1. Chat History View で、**[Advanced Filter]**（高度なフィルタ）アイコンをクリックします。

   [Advanced Filter]ダイアログ ボックスが表示されます。
2. **[Display only sessions within specified date range]**（指定した日付範囲内のセッションのみを表示）を選択します。
3. **[From date]**（以降の日）と**[To date]**（以前の日）の各ボックスに年月日を入力するか、カレンダの横の矢印をクリックして日付を選択します。
4. **[OK]**をクリックします。

初期設定フォルダ以外のフォルダに保存されているセッションの表示

1. Chat History View で、**[Advanced Filter]**アイコンをクリックします。
2. **[Use an alternate history files folder]**（別の履歴ファイル フォルダを使用）チェック ボックスにチェックを入れます。
3. フォルダの場所を入力するか、**[Browse]**（参照）をクリックしてフォルダを探します。
4. **[OK]**をクリックします。

高度なタスク

別のコンピュータへの Privacy Manager Certificate と Trusted Contact の移行

Privacy Manager Certificate と Trusted Contact を、安全に別のコンピュータに移行できます。これには、パスワードで保護されたファイルとして Privacy Manager Certificate と Trusted Contact をネットワーク上の場所かリムーバブル ストレージ デバイスにエクスポートしてから、新しいコンピュータにこのファイルをインポートします。

Privacy Manager Certificate と Trusted Contact のエクスポート

Privacy Manager Certificate と Trusted Contact をパスワードで保護されたファイルにエクスポートするには、以下の手順で操作します。

1. Privacy Manager を開き、**[Migration]**（移行）をクリックします。
2. **[Export migration file]**（移行ファイルのエクスポート）をクリックします。
3. [Select Data]（データの選択）ページで、移行ファイルに含めるデータのカテゴリを選択してから**[Next]**（次へ）をクリックします。
4. [Migration File]（移行ファイル）ページで、ファイル名を入力するか、**[Browse]**（参照）をクリックして場所を探し、**[Next]**（次へ）をクリックします。
5. パスワードの入力と確認を行い、**[Next]**（次へ）をクリックします。

注記：　移行ファイルをインポートするときに必要ですので、このパスワードは安全な場所に保管してください。

6. 選択したセキュリティ ログオン方法で認証します。
7. [Migration File Saved]（移行ファイルを保存しました）ページで、**[Finish]**（完了）をクリックします。

Privacy Manager Certificate と Trusted Contact のインポート

Privacy Manager Certificate と Trusted Contact をパスワードで保護されたファイルからインポートするには、以下の手順で操作します。

1. Privacy Manager を開き、**[Migration]**（移行）をクリックします。
2. **[Import migration file]**（移行ファイルのインポート）をクリックします。
3. [Select Data]（データの選択）ページで、移行ファイルに含めるデータのカテゴリを選択してから**[Next]**（次へ）をクリックします。
4. [Migration File]（移行ファイル）ページで、ファイル名を入力するか、**[Browse]**（参照）をクリックして場所を探し、**[Next]**（次へ）をクリックします。
5. [Migration File Imported]（移行ファイルをインポートしました）ページで、**[Finish]**（完了）をクリックします。

5 File Sanitizer for HP ProtectTools

File Sanitizer は、コンピュータ上のフォルダやファイル（個人情報やファイル、履歴データや Web 関連データ、その他のデータ コンポーネント）を安全にシュレッドしたり、ハードドライブを定期的に「ブリーチ（漂白）」したりすることができるツールです。

注記： File Sanitizer は現在、ハードドライブ上でのみ動作します。

シュレッドについて

Windows でフォルダやファイルを削除しても、そのフォルダやファイルの内容はハードドライブから完全に削除されません。Windows はフォルダやファイルの参照情報のみを削除します。他のフォルダやファイルによってハードドライブの同じ領域を新しい情報で上書きしないかぎり、フォルダやファイルの内容はハードドライブに引き続き残ったままとなります。

フォルダやファイルのシュレッドは、データの内容をわからなくするアルゴリズムが実行されて元のフォルダやファイルを取り戻すことが事実上不可能になる点で、通常の Windows の削除（File Sanitizer ではシンプル削除とも言います）とは異なります。

シュレッド プロファイル（[High Security]（セキュリティ設定、高）、[Medium Security]（セキュリティ設定、中）、または[Low Security]（セキュリティ設定、低）を選択すると、あらかじめ定義されているフォルダやファイルの一覧と消去方法がシュレッドのために自動で選択されます。また、シュレッド プロファイルをカスタマイズして、シュレッド サイクル数、シュレッド対象に含めるフォルダやファイル、シュレッド前に確認するフォルダやファイル、およびシュレッド対象から除外するフォルダやファイルを指定することもできます。

自動シュレッドのスケジュールを設定することができます。また、必要に応じていつでもフォルダやファイルを手動シュレッドすることもできます。

空き領域ブリーチを実行すると、削除されたフォルダやファイルに対してランダムなデータを安全に上書きできるため、削除されたフォルダやファイルの元の内容をユーザは参照できなくなります。

空き領域ブリーチについて

注記： 空き領域ブリーチは、Windows のゴミ箱を使用して削除したフォルダやファイル、または手動で削除したフォルダやファイルを対象とする機能です。空き領域ブリーチを実行しても、シュレッドされたフォルダやファイルにセキュリティが追加されることはありません。

タスクバーの右端の通知領域にある[HP ProtectTools]アイコンを使用して、空き領域ブリーチの自動スケジュールを有効にするか、空き領域ブリーチを手動で実行することができます。

セットアップ手順

File Sanitizer の起動

File Sanitizer を起動するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。
2. **[File Sanitizer]**をクリックします。

   または

- **[File Sanitizer]**アイコンをダブルクリックします。

  または

- タスクバーの右端の通知領域にある[HP ProtectTools]アイコンを右クリックしてから、[File Sanitizer]→[Open File Sanitizer]（File Sanitizer を開く）の順にクリックします。

シュレッド スケジュールの設定

1. **[File Sanitizer]**を起動して、**[Shred]**（シュレッド）をクリックします。
2. シュレッド オプションを以下の中から選択します。
   - **[Windows startup]**（Windows の起動時）：選択されているすべてのフォルダやファイルを Windows の起動時にシュレッドするには、このオプションを選択します。
   - **[Windows shutdown]**（Windows のシャットダウン時）：選択されているすべてのフォルダやファイルを Windows のシャットダウン時にシュレッドするには、このオプションを選択します。

     注記：　このオプションを選択すると、シャットダウン時にダイアログ ボックスが表示され、選択されているフォルダやファイルのシュレッドを実行するか、シュレッド処理を中止するかを確認します。シュレッド処理に進む場合は**[Yes]**（はい）、シュレッドを中止する場合は**[No]**（いいえ）をクリックします。
   - **[Web browser open]**（Web ブラウザの起動時）：ブラウザの URL 履歴など、選択されているすべての Windows 関連フォルダやファイルを Web ブラウザの起動時にシュレッドするには、このオプションを選択します。
   - **[Web browser quit]**（Web ブラウザの終了時）：ブラウザの URL 履歴など、選択されているすべての Windows 関連フォルダやファイルを Web ブラウザの終了時にシュレッドするには、このオプションを選択します。
   - **[Scheduler]**（スケジューラ）：[Activate Scheduler]（スケジューラの起動）チェック ボックスにチェックを入れ、Windows のパスワードを入力してから、選択されているフォルダやファイルをシュレッドする日付と時刻を入力します。
3. **[Apply]**（適用）→**[OK]**の順にクリックします。

空き領域ブリーチのスケジュール設定

注記： 空き領域ブリーチは、Windows のゴミ箱を使用して削除したフォルダやファイル、または手動で削除したフォルダやファイルを対象とする機能です。空き領域ブリーチを実行しても、シュレッドされたフォルダやファイルにセキュリティが追加されることはありません。

空き領域ブリーチのスケジュールを設定するには、以下の手順で操作します。

1. File Sanitizer を起動して、**[Free Space Bleaching]**（空き領域ブリーチ）をクリックします。
2. **[Activate Scheduler]**（スケジューラの起動）チェック ボックスにチェックを入れ、Windows のパスワードを入力してから、ハードドライブをブリーチする日付と時刻を入力します。
3. **[Apply]**→**[OK]**の順にクリックします。

   注記： 空き領域ブリーチ操作は、長い時間がかかる場合があります。空き領域ブリーチはバックグラウンドで実行されますが、プロセッサの使用量が大きくなるため、コンピュータの動作が遅くなる場合があります。

シュレッド プロファイルの選択または作成

あらかじめ定義されているプロファイルを選択するか、自分のプロファイルを作成して、消去方法を指定したりシュレッドするフォルダやファイルを選択したりすることができます。

あらかじめ定義されているシュレッド プロファイルの選択

あらかじめ定義されているシュレッド プロファイル（[High Security]（セキュリティ設定、高）、[Medium Security]（セキュリティ設定、中）または[Low Security]（セキュリティ設定、低）を選択すると、あらかじめ定義されている消去方法とフォルダやファイルの一覧が自動的に選択されます。[View Details]（詳細を表示）ボタンをクリックすると、シュレッド用に選択されているフォルダやファイルのあらかじめ定義されている一覧が表示されます。

あらかじめ定義されているシュレッド プロファイルを選択するには、以下の手順で操作します。

1. File Sanitizer を起動し、**[Settings]**（設定）をクリックします。
2. あらかじめ定義されているシュレッド プロファイルをクリックします。
3. **[View Details]**（詳細を表示）をクリックして、シュレッド用に選択されているフォルダやファイルの一覧を表示します。
4. **[Shred the following]**（次のフォルダ/ファイルをシュレッドする）で、シュレッド前に確認する各フォルダやファイルの横のチェック ボックスにチェックを入れます。
5. **[Cancel]**（キャンセル）→**[OK]**の順にクリックします。

シュレッド プロファイルのカスタマイズ

シュレッド プロファイルを作成するには、シュレッド サイクル数、シュレッド対象に含めるフォルダやファイル、シュレッド前に確認するフォルダやファイル、およびシュレッド対象から除外するフォルダやファイルを指定します。

1. File Sanitizer を起動し、**[Settings]**→**[Advanced Security Settings]**（高度なセキュリティ設定）→**[View Details]**（詳細を表示）の順にクリックします。

2. シュレッド サイクル数を指定します。

   注記： 各フォルダやファイルに対して、指定した数のシュレッド サイクルが実行されます。たとえば、シュレッド サイクルで 3 を選択すると、データの内容をわからなくするアルゴリズムが異なる 3 つの時間に実行されます。高いセキュリティ設定でシュレッド サイクルを選択すると、シュレッドに非常に長い時間がかかる場合があります。ただし、指定するシュレッド サイクル数を大きくするほど、コンピュータのセキュリティは高まります。

3. シュレッドするフォルダやファイルを選択するには、以下の手順で操作します。

   a. **[Available shred options]**（使用できるシュレッド オプション）で、フォルダやファイルをクリックしてから**[Add]**（追加）をクリックします。

   b. カスタム フォルダやファイルを追加するには、[Add Custom Option]（カスタムオプションの追加）をクリックし、ファイル名またはフォルダ名を入力して**[OK]**をクリックします。カスタム フォルダやファイルをクリックして、**[Add]**をクリックします。

      注記： 使用できるシュレッド オプションからフォルダやファイルを削除するには、フォルダやファイルをクリックしてから**[Delete]**（削除）をクリックします。

4. **[Shred the following]**（次のフォルダ/ファイルをシュレッドする）で、シュレッド前に確認する各フォルダやファイルの横のチェック ボックスにチェックを入れます。

   注記： シュレッド リストからフォルダやファイルを削除するには、フォルダやファイルをクリックしてから**[Remove]**（削除）をクリックします。

5. **[Do not shred the following]**（次のフォルダ/ファイルをシュレッドしない）で、**[Add]**をクリックして、シュレッド対象から除外するフォルダやファイルを指定します。

   注記： ファイルの拡張子のみを指定して、シュレッド対象から除外することができます。たとえば、.BMP ファイル拡張子を追加すると、.BMP 拡張子を持つすべてのファイルが削除対象から除外されます。

   除外リストからフォルダやファイルを削除するには、フォルダやファイルをクリックしてから**[Delete]**をクリックします。

6. シュレッド プロファイルの設定を完了したら、**[Apply]**→**[OK]**の順にクリックします。

シンプル削除プロファイルのカスタマイズ

シンプル削除プロファイルは、シュレッドしないで標準的なフォルダやファイルの削除を実行します。シンプル削除プロファイルをカスタマイズするには、シンプル削除対象に含めるフォルダやファイル、シンプル削除の実行前に確認するフォルダやファイル、およびシンプル削除対象から除外するフォルダやファイルを指定します。

注記： シンプル削除オプションを使用する場合は、空き領域ブリーチを定期的に実行することを強くおすすめします。

1. File Sanitizer を起動し、**[Settings]**（設定）→**[Simple Delete Setting]**（シンプル削除設定）→**[View Details]**（詳細を表示）の順にクリックします。

2. 削除するフォルダやファイルを選択するには、以下の手順で操作します。

   a. **[Available delete options]**（使用できる削除オプション）で、フォルダやファイルをクリックしてから**[Add]**（追加）をクリックします。

   b. カスタム フォルダやファイルを追加するには、**[Add Custom Option]**（カスタムオプションの追加）をクリックし、ファイル名またはフォルダ名を入力して**[OK]**をクリックします。カスタム フォルダやファイルをクリックして、**[Add]**をクリックします。

   注記： 使用できる削除オプションからフォルダやファイルを削除するには、フォルダやファイルをクリックしてから**[Delete]**（削除）をクリックします。

3. **[Delete the following]**（次のフォルダ/ファイルを削除する）で、削除前に確認する各フォルダやファイルの横のチェック ボックスにチェックを入れます。

   注記： 削除リストからフォルダやファイルを削除するには、フォルダやファイルをクリックしてから**[Remove]**（削除）をクリックします。

4. **[Do not shred the following]**（次のフォルダ/ファイルをシュレッドしない）で、**[Add]**をクリックして、シュレッド対象から除外するフォルダやファイルを指定します。

   注記： ファイルの拡張子のみを指定して、削除対象から除外することができます。たとえば、.BMP ファイル拡張子を追加すると、.BMP 拡張子を持つすべてのファイルが削除対象から除外されます。

   除外リストからフォルダやファイルを削除するには、フォルダやファイルをクリックしてから**[Delete]**をクリックします。

5. シンプル削除プロファイルの設定を完了したら、**[Apply]**（適用）→**[OK]**の順にクリックします。

シュレッド スケジュールの設定

1. File Sanitizer を起動して、**[Shred]**（シュレッド）をクリックします。

2. シュレッド オプションを以下の中から選択します。

   - **[Windows startup]**（Windows の起動時）：選択されているすべてのフォルダやファイルを Windows の起動時にシュレッドするには、このオプションを選択します。

   - **[Windows shutdown]**（Windows のシャットダウン時）：選択されているすべてのフォルダやファイルを Windows のシャットダウン時にシュレッドするには、このオプションを選択します。

     注記： このオプションを選択すると、シャットダウン時にダイアログ ボックスが表示され、選択されているフォルダやファイルのシュレッドを実行するか、シュレッド処理を中止するかを確認します。シュレッド処理に進む場合は[Yes]（はい）、シュレッドを中止する場合は[No]（いいえ）をクリックします。

   - **[Web browser open]**（Web ブラウザの起動時）：ブラウザの URL 履歴など、選択されているすべての Windows 関連フォルダやファイルを Web ブラウザの起動時にシュレッドするには、このオプションを選択します。

- **[Web browser quit]**（Web ブラウザの終了時）：ブラウザの URL 履歴など、選択されているすべての Windows 関連フォルダやファイルを Web ブラウザの終了時にシュレッドするには、このオプションを選択します。
- **[Scheduler]**（スケジューラ）：[Activate Scheduler]（スケジューラの起動）チェック ボックスにチェックを入れ、Windows のパスワードを入力してから、選択されているフォルダやファイルをシュレッドする日付と時刻を入力します。

3. **[Apply]**（適用）→**[OK]**の順にクリックします。

空き領域ブリーチのスケジュール設定

注記： 空き領域ブリーチは、Windows のゴミ箱を使用して削除したフォルダやファイル、または手動で削除したフォルダやファイルを対象とする機能です。空き領域ブリーチを実行しても、シュレッドされたフォルダやファイルにセキュリティが追加されることはありません。

空き領域ブリーチのスケジュールを設定するには、以下の手順で操作します。

1. File Sanitizer を起動して、**[Free Space Bleaching]**（空き領域ブリーチ）をクリックします。
2. **[Activate Scheduler]**（スケジューラの起動）チェック ボックスにチェックを入れ、Windows のパスワードを入力してから、ハードドライブをブリーチする日付と時刻を入力します。
3. **[Apply]**（適用）→**[OK]**の順にクリックします。

   注記： 空き領域ブリーチ操作は、長い時間がかかる場合があります。空き領域ブリーチはバックグラウンドで実行されますが、プロセッサの使用量が大きくなるため、コンピュータの動作が遅くなる場合があります。

シュレッド プロファイルの選択または作成

あらかじめ定義されているシュレッド プロファイルの選択

あらかじめ定義されているシュレッド プロファイル（[High Security]（セキュリティ設定、高）、[Medium Security]（セキュリティ設定、中）または[Low Security]（セキュリティ設定、低）を選択すると、あらかじめ定義されている消去方法とフォルダやファイルの一覧が自動的に選択されます。[View Details]（詳細を表示）ボタンをクリックすると、シュレッド用に選択されているフォルダやファイルのあらかじめ定義されている一覧が表示されます。

あらかじめ定義されているシュレッド プロファイルを選択するには、以下の手順で操作します。

1. File Sanitizer を起動し、**[Settings]**（設定）をクリックします。
2. あらかじめ定義されているシュレッド プロファイルをクリックします。
3. **[View Details]**（詳細を表示）をクリックして、シュレッド用に選択されているフォルダやファイルの一覧を表示します。
4. **[Shred the following]**（次のフォルダ/ファイルをシュレッドする）で、シュレッド前に確認する各フォルダやファイルの横のチェック ボックスにチェックを入れます。
5. **[Cancel]**（キャンセル）→**[OK]**の順にクリックします。

シュレッド プロファイルのカスタマイズ

シュレッド プロファイルを作成するには、シュレッド サイクル数、シュレッド対象に含めるフォルダやファイル、シュレッド前に確認するフォルダやファイル、およびシュレッド対象から除外するフォルダやファイルを指定します。

1. File Sanitizer を起動し、**[Settings]**→**[Advanced Security Settings]**（高度なセキュリティ設定）→**[View Details]**（詳細を表示）の順にクリックします。
2. シュレッド サイクル数を指定します。

   注記： 各フォルダやファイルに対して、指定した数のシュレッド サイクルが実行されます。たとえば、シュレッド サイクルで 3 を選択すると、データの内容をわからなくするアルゴリズムが異なる 3 つの時間に実行されます。高いセキュリティ設定でシュレッド サイクルを選択すると、シュレッドに非常に長い時間がかかる場合があります。ただし、指定するシュレッド サイクル数を大きくするほど、コンピュータのセキュリティは高まります。

3. シュレッドするフォルダやファイルを選択するには、以下の手順で操作します。
   a. **[Available shred options]**（使用できるシュレッド オプション）で、フォルダやファイルをクリックしてから**[Add]**（追加）をクリックします。
   b. カスタム フォルダやファイルを追加するには、[Add Custom Option]（カスタムオプションの追加）をクリックし、ファイル名またはフォルダ名を入力して**[OK]**をクリックします。カスタム フォルダやファイルをクリックして、**[Add]**をクリックします。

      注記： 使用できるシュレッド オプションからフォルダやファイルを削除するには、フォルダやファイルをクリックしてから**[Delete]**（削除）をクリックします。

4. **[Shred the following]**（次のフォルダ/ファイルをシュレッドする）で、シュレッド前に確認する各フォルダやファイルの横のチェック ボックスにチェックを入れます。

   注記： シュレッド リストからフォルダやファイルを削除するには、フォルダやファイルをクリックしてから**[Remove]**（削除）をクリックします。

5. **[Do not shred the following]**（次のフォルダ/ファイルをシュレッドしない）で、**[Add]**をクリックして、シュレッド対象から除外するフォルダやファイルを指定します。

   注記： ファイルの拡張子のみを指定して、シュレッド対象から除外することができます。たとえば、.BMP ファイル拡張子を追加すると、.BMP 拡張子を持つすべてのファイルが削除対象から除外されます。

   除外リストからフォルダやファイルを削除するには、フォルダやファイルをクリックしてから**[Delete]**をクリックします。

6. シュレッド プロファイルの設定を完了したら、**[Apply]**（適用）→**[OK]**の順にクリックします。

シンプル削除プロファイルのカスタマイズ

シンプル削除プロファイルは、シュレッドしないで標準的なフォルダやファイルの削除を実行します。シンプル削除プロファイルをカスタマイズするには、シンプル削除対象に含めるフォルダやファイル、シンプル削除の実行前に確認するフォルダやファイル、およびシンプル削除対象から除外するフォルダやファイルを指定します。

注記： シンプル削除オプションを使用する場合は、空き領域ブリーチを定期的に実行することを強くおすすめします。

1. File Sanitizer を起動し、**[Settings]**（設定）→**[Simple Delete Setting]**（シンプル削除設定）→**[View Details]**（詳細を表示）の順にクリックします。
2. 削除するフォルダやファイルを選択するには、以下の手順で操作します。
   - **[Available delete options]**（使用できる削除オプション）で、フォルダやファイルをクリックしてから**[Add]**（追加）をクリックします。
   - カスタム フォルダやファイルを追加するには、**[Add Custom Option]**（カスタムオプションの追加）をクリックし、ファイル名またはフォルダ名を入力して**[OK]**をクリックします。カスタム フォルダやファイルをクリックして、**[Add]**をクリックします。

   注記： 使用できる削除オプションからフォルダやファイルを削除するには、フォルダやファイルをクリックしてから**[Delete]**（削除）をクリックします。
3. **[Delete the following]**（次のフォルダ/ファイルを削除する）で、削除前に確認する各フォルダやファイルの横のチェック ボックスにチェックを入れます。

   注記： 削除リストからフォルダやファイルを削除するには、フォルダやファイルをクリックしてから**[Remove]**（削除）をクリックします。
4. **[Do not delete the following]**（次のフォルダ/ファイルを削除しない）で、**[Add]**をクリックして、削除対象から除外するフォルダやファイルを指定します。

   注記： ファイルの拡張子のみを指定して、削除対象から除外することができます。たとえば、.BMP ファイル拡張子を追加すると、.BMP 拡張子を持つすべてのファイルが削除対象から除外されます。

   除外リストからフォルダやファイルを削除するには、フォルダやファイルをクリックしてから**[Delete]**をクリックします。
5. シンプル削除プロファイルの設定を完了したら、**[Apply]**（適用）→**[OK]**の順にクリックします。

一般的なタスク

キーの組み合わせによるシュレッドの開始

キーの組み合わせを指定するには、以下の手順で操作します。

1. File Sanitizer を起動して、**[Shred]**（シュレッド）をクリックします。
2. **[Key sequence]**（キーの組み合わせ）チェック ボックスにチェックを入れます。
3. 使用できるボックスに文字を 1 つ入力してから、**[CTRL]**ボックス、**[ALT]**ボックス、または**[SHIFT]**ボックスのどれかまたは 3 つすべてにチェックを入れます。

   たとえば、s キーと ctrl + shift キーを使用して自動シュレッドを開始するには、ボックスに s と入力してから、**[CTRL]**オプションと**[SHIFT]**オプションにチェックを入れます。

注記： 設定済みの他のキーの組み合わせとは異なるキーの組み合わせを選択してください。

キーの組み合わせでシュレッドを開始するには、以下の手順で操作します。

1. ctrl キー、alt キー、または shift キー（または指定した組み合わせのキー）を押しながら、選択した文字キーを押します。
2. 確認用のダイアログ ボックスが表示されたら、**[Yes]**（はい）をクリックします。

[File Sanitizer]アイコンの使用

△ **注意：** シュレッドしたフォルダやファイルは復元できません。手動でシュレッドするために選択するフォルダやファイルについては、十分に検討してください。

1. シュレッドするドキュメントまたはフォルダに移動します。
2. シュレッドするフォルダやファイルをデスクトップの[File Sanitizer]アイコンにドラッグします。
3. 確認用のダイアログ ボックスが表示されたら、**[Yes]**（はい）をクリックします。

単一フォルダやファイルの手動シュレッド

△ **注意：** シュレッドしたフォルダやファイルは復元できません。手動でシュレッドするために選択するフォルダやファイルについては、十分に検討してください。

1. タスクバーの右端の通知領域にある**[HP ProtectTools]**アイコンを右クリックしてから、**[File Sanitizer]**→**[Shred One]**（単一フォルダ/ファイルをシュレッド）の順にクリックします。
2. [Browse]（参照）ダイアログ ボックスが開いたら、シュレッドするフォルダやファイルに移動してから**[OK]**をクリックします。

   注記： 選択できるフォルダやファイルは、単一のファイルまたはフォルダです。

3. 確認用のダイアログ ボックスが表示されたら、**[Yes]**（はい）をクリックします。

または

1. デスクトップにある**[File Sanitizer]**アイコンを右クリックしてから、**[Shred One]**をクリックします。
2. [Browse]ダイアログ ボックスが開いたら、シュレッドするフォルダやファイルに移動してから**[OK]**をクリックします。
3. 確認用のダイアログ ボックスが表示されたら、**[Yes]**（はい）をクリックします。

または

1. File Sanitizer を起動して、**[Shred]**（シュレッド）をクリックします。
2. **[Browse]**（参照）ボタンをクリックします。
3. [Browse]ダイアログ ボックスが開いたら、シュレッドするフォルダやファイルに移動してから**[OK]**をクリックします。
4. 確認用のダイアログ ボックスが表示されたら、**[Yes]**（はい）をクリックします。

または

1. File Sanitizer を起動して、**[Shred]**（シュレッド）をクリックします。
2. **[Shred Now]**（今すぐシュレッド）ボタンをクリックします。
3. 確認用のダイアログ ボックスが表示されたら、**[Yes]**（はい）をクリックします。

選択されているすべてのフォルダやファイルの手動シュレッド

1. タスクバーの右端の通知領域にある**[HP ProtectTools]**アイコンを右クリックしてから、**[File Sanitizer]→[Shred Now]**（今すぐシュレッド）の順にクリックします。
2. 確認用のダイアログ ボックスが表示されたら、**[Yes]**（はい）をクリックします。

   または

1. デスクトップにある**[File Sanitizer]**アイコンを右クリックしてから、**[Shred Now]**をクリックします。
2. 確認用のダイアログ ボックスが表示されたら、**[Yes]**（はい）をクリックします。

空き領域ブリーチの手動実行

1. タスクバーの右端の通知領域にある**[HP ProtectTools]**アイコンを右クリックしてから、**[File Sanitizer]→[Bleach Now]**（今すぐブリーチ）の順にクリックします。
2. 確認用のダイアログ ボックスが表示されたら、**[Yes]**（はい）をクリックします。

または

1. File Sanitizer を起動して、**[Free Space Bleaching]**（空き領域ブリーチ）をクリックします。
2. **[Bleach Now]**をクリックします。
3. 確認用のダイアログ ボックスが表示されたら、**[Yes]**（はい）をクリックします。

シュレッド操作または空き領域ブリーチ操作の停止

シュレッド操作または空き領域ブリーチ操作の実行中、通知領域にある[HP ProtectTools Security Manager]（HP ProtectTools セキュリティ マネージャ）アイコンの上にメッセージが表示されます。このメッセージには、シュレッド処理または空き領域ブリーチ処理の詳細（完了した割合）と、操作を停止するためのオプションが表示されます。

この操作を停止するには、以下の手順で操作します。

▲ メッセージをクリックしてから**[Stop]**（停止）ボタンをクリックすると、操作がキャンセルされます。

ログ ファイルの表示

シュレッド操作または空き領域ブリーチ操作を実行するたびに、エラーのログ ファイルまたは障害のログ ファイルが生成されます。これらのログ ファイルは、最新のシュレッド操作または空き領域ブリーチ操作に従って常に更新されます。

注記： 正常にシュレッドまたはブリーチされたファイルは、ログ ファイルには表示されません。

ログ ファイルには、シュレッド操作について作成されるファイルと空き領域ブリーチ操作について作成されるファイルがあります。これらのログ ファイルは、ハードドライブ上の以下の場所に存在します。

- C:¥Program Files¥Hewlett-Packard¥File Sanitizer¥[Username]（ユーザ名）_ShredderLog.txt
- C:¥Program Files¥Hewlett-Packard¥File Sanitizer¥[Username]_DiskBleachLog.txt

6 BIOS Configuration for HP ProtectTools

BIOS Configuration for HP ProtectTools を使用すると、[Computer Setup]ユーティリティのセキュリティ設定にアクセスできます。これによって、[Computer Setup]で管理されるシステムのセキュリティ機能に Windows から簡単にアクセスできるようになります。

BIOS Configuration を使用すると、以下のことを行えます。

- 管理者パスワードを管理できます。
- 内蔵セキュリティ認証など、電源投入時のその他の認証機能を設定できます。
- CD-ROM のブートやハードウェア ポートなど、ハードウェア機能を有効および無効に設定できます。
- マルチブートの有効化および起動順序の変更を含む、ブート オプションを設定できます。

注記： BIOS Configuration for HP ProtectTools にある機能の多くは、[Computer Setup]でも使用できます。

一般的なタスク

BIOS Configuration を使用すると、通常は起動時に f10 キーを押して[Computer Setup]を使用することでしかアクセスできない、各種のコンピュータ設定を管理できます。

BIOS Configuration へのアクセス

BIOS Configuration にアクセスするには、以下の手順で操作します。

1. **[スタート]**→**[Settings]**（設定）→**[コントロール パネル]**の順にクリックします。
2. **[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）→**[BIOS Configuration]**の順にクリックします。

   タスクバーの右端の通知領域にあるアイコンから BIOS Configuration にアクセスすることもできます。

   注記： [HP ProtectTools Security Manager]アイコンを表示するには、通知領域内の**[Show Hidden Icons]**（隠れているインジケータを表示します）アイコン（**[<]**または**[<<]**）をクリックする必要があります。

   - 通知領域内の**[HP ProtectTools Security Manager]**アイコンを右クリックします。
   - **[BIOS Configuration]**をクリックします。
3. HP ProtectTools ユーザの場合は、Windows パスワードを入力します。
   - Windows パスワードが正しく入力されていても、BIOS 管理者ではない場合、変更機能はセキュリティ レベルの設定によって異なります。詳しくは、68 ページの 「システム コンフィギュレーション オプションの設定」を参照してください。

     注記： HP ProtectTools ユーザは、BIOS 管理者である場合とそうでない場合があります。
   - Windows パスワードが正しく入力されなかった場合、BIOS コンフィギュレーション設定の表示のみ可能で、変更することはできません。
4. HP ProtectTools ユーザではない場合、BIOS Configuration ソフトウェアは BIOS 管理者パスワードが設定されているかどうかを確認します。
   - BIOS 管理者パスワードが設定されている場合、そのパスワードを入力する必要があります。
     - BIOS 管理者パスワードを正しく入力すると、BIOS コンフィギュレーション設定の表示と変更ができるようになります。
     - BIOS 管理者パスワードが設定されているが、そのパスワードが入力されなかったか、または正しく入力されなかった場合、BIOS コンフィギュレーション設定を表示できますが、変更することはできません。
   - BIOS 管理者パスワードが設定されていない場合、BIOS コンフィギュレーション設定の表示および変更の両方を実行できます。

設定の表示または変更

コンフィギュレーション設定を表示または変更するには、以下の手順で操作します。

1. 以下の BIOS Configuration ページのどれかを使用します。
   - [File]（ファイル）
   - [Security]（セキュリティ）
   - [System Configuration]（システム コンフィギュレーション）
2. 変更を行った後、**[Apply]**（適用）をクリックし、変更を保存して、ウィンドウを開いたままにします。

   または

   変更を行った後、**[OK]**をクリックし、変更を保存して、ウィンドウを閉じます。
3. 終了してコンピュータを再起動します。

   変更した内容はコンピュータの再起動時に有効になります。

注記： パスワードの変更はただちに有効になります。コンピュータを再起動する必要はありません。

システム情報の表示

[File]（ファイル）ページを使用して、以下の種類の情報を表示します。

- コンピュータ（シリアル番号を含む）およびシステム内のバッテリについての識別情報
- プロセッサ、キャッシュ サイズおよびメモリ サイズ、ビデオのバージョン、キーボード コントローラのバージョン、およびシステム ROM についての仕様情報

注記： [File]ページの情報は表示のみ可能です。表示されている情報は変更できません。

システム情報を表示するには、以下の手順で操作します。

▲ [BIOS Configuration]にアクセスして**[File]**（ファイル）をクリックします。

高度なタスク

セキュリティ オプションの設定

BIOS Configuration の[Security]（セキュリティ）ページを使用して、コンピュータのセキュリティを強化します。

注記： すべてのオプションがすべてのコンピュータで使用できるとは限りません。また、追加のオプションが含まれる可能性もあります。

セキュリティ オプションを設定するには、以下の手順で操作します。

1. [BIOS Configuration]にアクセスし、**[Security]**をクリックします。
2. 以下の表にあるオプションのどれかを選択します。
3. 必要に応じて設定を変更します。
4. **[Apply]**（適用）をクリックして、新しい設定を適用し、ウィンドウを開いたままにします。

   または

   [OK]をクリックして、新しい設定を適用し、ウィンドウを閉じます。

[Security]（セキュリティ）

オプション	操作
[BIOS Administrator Password]（BIOS 管理者パスワード） **注記：** このオプションは、[Setup Password]（セットアップ パスワード）と呼ばれる場合があります。	**[Set]**（設定）ボタンをクリックして、BIOS 管理者パスワードを設定します。

System IDs（システム ID）

オプション	操作
[Ownership Tag]（所有者タグ）	入力、表示、または変更します。
[Asset Tracking Number]（アセット タグ）	入力、表示、または変更します。

TPM Embedded Security（TPM 内蔵セキュリティ）

注記： この機能は、HP ProtectTools 内蔵セキュリティ チップ（TPM）が装備されているコンピュータでのみサポートされます。

オプション	操作
[Reset of TPM from OS]（OS からの TPM のリセット）	有効または無効にします。
[OS Management of TPM]（TPM の OS 管理）	有効または無効にします。
[Embedded Security Device Availability]（内蔵セキュリティ デバイスの有無）	使用可能にするか、非表示にするかを選択します。
[Power-On Authentication Support]（電源投入時認証サポート）	スマート カードの電源投入時認証のサポートを有効/無効にします。

オプション	操作
	注記： この機能はオプションのスマート カード リーダーを搭載したコンピュータでのみサポートされます。
[Automatic Drivelock Support]（自動 Drivelock サポート）	有効または無効にします。

Administrator Tools（管理者ツール）

オプション	操作
[HP SpareKey]	有効または無効にします。
[Fingerprint Reset on Reboot]（再起動時に指紋認証をリセット（存在する場合））	有効または無効にします。

Password Policy（パスワード ポリシー）

オプション	操作
[At least one symbol required]（記号を必ず含める）	有効または無効にします。
[At least one number required]（数字を必ず含める）	有効または無効にします。
[At least one upper case character required]（大文字の英字を必ず含める）	有効または無効にします。
[At least one lower case character required]（小文字の英字を必ず含める）	有効または無効にします。
[Are spaces allowed in password]（パスワードに空白文字を許可しますか）	有効または無効にします。

Hard Disk Sanitization Report（ハードディスクのクリーンアップ レポート）

オプション	操作
[Hard Disk Sanitization]（ハードディスクのクリーンアップ）	すでに 1 回以上、ハードディスクのクリーンアップが実行されている場合、コンピュータ上で完了した最も最近実行されたハードディスクのクリーンアップ手順についての情報を表示します。 注記： このオプションを使用すると、コンピュータのハードドライブから重要なデータが削除されます。ハードドライブをクリーンアップし、その後コンピュータから削除しても、クリーンアップ プロセスの情報はまだ使用可能です。

システム コンフィギュレーション オプションの設定

[System Configuration]（システム コンフィギュレーション）ページでは、システム コンフィギュレーション設定の表示と設定の変更ができます。

注記： すべてのオプションがすべてのコンピュータで使用できるとは限りません。また、追加のオプションが含まれる可能性もあります。

システム コンフィギュレーション オプションを設定するには、以下の手順で操作します。

1. **[BIOS Configuration]**にアクセスし、**[System Configuration]**（システム コンフィギュレーション）をクリックします。
2. 以下の表で説明されているオプションのどれかを選択します。
   - **[Port options]**（ポート オプション）
   - **[Boot options]**（ブート オプション）
   - **[Device configuration options]**（デバイス コンフィギュレーション オプション）
   - **[Built-in device options]**（内蔵デバイス オプション）
   - **[AMT options]**（AMT オプション）（一部のモデルのみ）
   - **[Security level options]**（セキュリティ レベル オプション）
3. 必要に応じて設定を変更します。
4. **[Apply]**（適用）をクリックして、新しい設定をシステムに適用し、ウィンドウを開いたままにします。

   または

   [HP ProtectTools Security Manager]（HP ProtectTools セキュリティ マネージャ）ウィンドウで**[OK]**をクリックして、新しい設定をシステムに適用し、ウィンドウを閉じます。

Port options（ポート オプション）

オプション	操作
[Flash Media Reader]（フラッシュ メディア リーダー）	有効または無効にします。
[USB Port]（USB ポート）	有効または無効にします。
[1394 port]（1394 ポート）	有効または無効にします。
[Express Card slot]（ExpressCard スロット）	有効または無効にします。

Boot options（ブート オプション）

オプション	操作
[Startup Check Delay (Sec)]（起動チェック遅延（秒））	[Startup Check]（起動チェック）の遅延を秒単位で設定します。
[Custom Logo]（カスタム ロゴ）	有効または無効にします。
[Express Boot Popup Delay (Sec)]（高速ブート ポップアップ遅延（秒））	[Express Boot Popup Delay]（高速ブート ポップアップ遅延）を秒単位で設定します。
[CD-ROM Boot]（CD-ROM ブート）	有効または無効にします。
[SD Card Boot]（SD カード ブート）	有効または無効にします。
[Boot from EFI File]（EFI ファイルからブート）	有効または無効にします。
[Floppy boot]（フロッピーディスク ブート）	有効または無効にします。

オプション	操作
[PXE Internal NIC boot]（PXE 内蔵 NIC ブート）	有効または無効にします。
[Boot Order]（ブート順序）	システム デバイスのブート順序を設定します。

Device configuration options（デバイス コンフィギュレーション オプション）

オプション	操作
[USB Legacy Support]（USB レガシー サポート）	有効または無効にします。
[Parallel port mode]（パラレル ポート モード）	パラレル ポートのモードを、標準モード、双方向モード、EPP（Enhanced Parallel Port）モード、または ECP（Enhanced Capabilities Port）モードから選択します。
[Fan Always on While on AC Power]（外部電源の使用時はファンを常にオン）	外部電源使用時のシステム ファンを有効または無効にします。
[Data Execution Prevention]（データ実行防止）	メモリ使用状況を監視し、疑わしいプログラムをシャットダウンするオプションを有効または無効にします。
SATA device mode（SATA デバイス モード）	IDE、AHCI、または RAID を選択します。
[Dual core CPU]（デュアル コア CPU）	有効または無効にします。
[Secondary battery fast charge]（セカンダリ バッテリ高速充電）	有効または無効にします。
[HP QuickLook 2]	有効または無効にします。
[TXT technology]（TXT テクノロジ）	有効または無効にします。
[Display Diagnostic URL]（診断 URL の表示）	有効または無効にします。
[HDD Translation Mode]（HDD 変換モード）	ビットシフトまたは LBA 支援を選択します。
[Virtualization technology]（仮想化テクノロジ）	同じコンピュータ上で複数の仮想マシンを並行して実行できるオプションを有効または無効にします。

Built-in device options（内蔵デバイス オプション）

オプション	操作
[Wireless Button State]（無線ボタン状態）	有効または無効にします。
[Embedded WWAN Device Radio]（内蔵無線 WAN デバイスの無線）	有効または無効にします。
[Fingerprint Device]（指紋認証デバイス）	有効または無効にします。
[Notebook MultiBay]（コンピュータ本体のマルチベイ）	有効または無効にします。
[Network Interface Controller (LAN)]（ネットワーク インタフェース コントローラ（LAN））	有効または無効にします。
[Ambient light sensor]（周辺光センサ）	有効または無効にします。

オプション	操作
[Embedded Bluetooth® Device Radio]（内蔵 Bluetooth デバイスの無線）	有効または無効にします。
[Wake on LAN]（ウェイク オン LAN）	同じネットワーク上の別のコンピュータから、使用するコンピュータの電源をリモートでオンにするオプションを有効または無効にします。

AMT options（AMT オプション）（一部のモデルのみ）

オプション	操作
[Terminal Emulation Mode]（ターミナル エミュレーション モード）	ANSI または VT100 を選択します。
[Firmware Verbosity]（ファームウェア詳細出力）	有効または無効にします。
[Firmware Progress Event Support]（ファームウェア進捗イベント サポート）	有効または無効にします。
[Unconfigure AMT on next boot]（次回ブート時に AMT を構成解除）	有効または無効にします。

Security level options（セキュリティ レベル オプション）

注記： これらの設定によって、HP ProtectTools ユーザのアクセス レベルを制御します。

オプション	操作
[CD-ROM Boot Security Level]（[CD-ROM ドライブ ブート]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Floppy Boot Security Level]（[フロッピーディスク ドライブからのブート]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Internal Network Adapter Boot Security Level]（[内蔵ネットワーク アダプタ ブート]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[USB Legacy Support Security Level]（[USB レガシー サポート]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Fan Always on While on AC Power Security Level]（[外部電源の使用中は常にファンをオンにする]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Flash Media Reader Security Level]（[フラッシュ メディア リーダー]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Startup Check Delay (Sec) Security Level]（[起動チェック遅延（秒）]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Parallel Port Mode Security Level]（[パラレル ポート モード]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Express Boot Popup Delay (Sec) Security Level]（[高速ブート ポップアップ遅延（秒）]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。

[LAN/WLAN Switching Security Level]（[LAN/無線 LAN 切り替え]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Embedded Bluetooth Device Radio Security Level]（[内蔵 Bluetooth デバイスの無線]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Embedded WWAN Device Radio Security Level]（[内蔵無線 WAN デバイスの無線]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Power-On Authentication Support Security Level]（[電源投入時認証サポート]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Automatic Drivelock Support Security Level]（[自動 Drivelock サポート]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Data Execution Prevention Security Level]（[データ実行防止]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[SATA Device Mode Security Level]（[SATA デバイス モード]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[USB Ports Security Level]（[USB ポート]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[1394 Port Security Level]（[1394 ポート]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Express Card Slot Security Level]（[ExpressCard スロット]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Dual Core CPU Security Level]（[デュアル コア CPU]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Wake on LAN Security Level]（[Wake on LAN]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Ambient Light Sensor Security Level]（[周辺光センサ]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Secondary Battery Fast Charge Security Level]（[セカンダリ バッテリ高速充電]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Embedded Security Device Availability Security Level]（[内蔵セキュリティ デバイス]の有無のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[HDD Translation Mode Security Level]（[HDD 変換モード]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Fingerprint Device Security Level]（[指紋認証デバイス]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Optical Disk Drive Security Level]（[オプティカル ドライブ]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Network Interface Controller (LAN) Security Level]（[ネットワーク インタフェース コントローラ（LAN）]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[OS Management of TPM Security Level]（[TPM の OS 管理]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Reset of TPM from OS Security Level]（[OS からの TPM のリセット]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。

[Virtualization Technology Security Level]（[Virtualization Technology]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Terminal Emulation Mode Security Level]（[ターミナル エミュレーション モード]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Firmware Verbosity Security Level]（[ファームウェア詳細]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Firmware Progress Event Support Security Level]（[ファームウェア進行イベント サポート]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Unconfigure AMT Security Level]（[AMT の構成解除]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Asset Tracking Number Security Level]（[アセット トラッキング番号]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Ownership Tag Security Level]（[オーナーシップタグ]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Boot Order Security Level]（[ブート順序]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Custom Logo Policy]（カスタム ロゴ ポリシー）	変更、または表示/非表示を切り替えます。
[Unconfigure AMT on next boot Security Level]（[次回ブート時に AMT を構成解除]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[SD Card Boot Security Level]（[SD カード ブートからのブート]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Boot From EFI File Security Level]（[EFI ファイルからブート]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[HP QuickLook 2 Security Level]（[HP QuickLook 2]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Wireless Button State Security Level]（[無線ボタン状態]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Modem Device Security Level]（[モデム デバイス]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Finger Print reset Security Level]（[指紋認証リセット]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[HP SpareKey Security Level]（[HP SpareKey]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[TXT Technology Security Level]（[TXT テクノロジ]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。
[Diagnostic URL Security Level]（[診断 URL]のセキュリティ レベル）	変更、または表示/非表示を切り替えます。

7 Embedded Security for HP ProtectTools（一部のモデルのみ）

注記： Embedded Security for HP ProtectTools を使用するには、統合された TPM（Trusted Platform Module）セキュリティ チップがコンピュータに内蔵されている必要があります。

Embedded Security for HP ProtectTools は、ユーザ データや証明情報を不正なアクセスから保護します。このソフトウェア モジュールには、以下のセキュリティ機能があります。

- 高度な Microsoft® EFS（Encryption File System）ファイルおよびフォルダの暗号化
- ユーザ データを保護するための PSD（Personal Secure Drive）の作成
- データ管理機能（キー階層のバックアップや復元など）
- Embedded Security ソフトウェアの使用時にデジタル証明情報の操作を保護するための他社製のアプリケーション（Microsoft Outlook や Internet Explorer など）のサポート

TPM 内蔵セキュリティ チップを使用すると、HP ProtectTools セキュリティマネージャの他のセキュリティ機能を強化したり有効にしたりできます。たとえば、Credential Manager for HP ProtectTools では、内蔵チップを Windows へのログオン時の認証要素として使用できます。一部のモデルでは、TPM 内蔵セキュリティ チップを使用して、BIOS Configuration for HP ProtectTools からアクセスする高度な BIOS セキュリティ機能を有効にすることもできます。

セットアップ手順

△ **注意：** セキュリティ上の危険にさらされないようにするために、IT 管理者が内蔵セキュリティ チップをただちに初期化することを強くおすすめします。内蔵セキュリティ チップを初期化しない場合、不正なユーザ、コンピュータ ワーム、またはウィルスがコンピュータのオーナシップを奪い、緊急リカバリ アーカイブの処理やユーザ アクセスの設定など所有者のタスクを制御してしまう可能性があります。

以下の 2 つの項目の手順に沿って操作し、内蔵セキュリティ チップを有効にして初期化します。

内蔵セキュリティ チップの有効化

内蔵セキュリティ チップは、[Computer Setup]ユーティリティで有効にする必要があります。この手順は、BIOS Configuration for HP ProtectTools では実行できません。

内蔵セキュリティ チップを有効にするには、以下の手順で操作します。

1. コンピュータの電源を入れるか再起動し、画面の左下隅に[F10 = ROM Based Setup]（ROM ベースのセットアップ）というメッセージが表示されている間に f10 キーを押して、[Computer Setup]を起動します。
2. 管理者パスワードを設定していない場合は、矢印キーを使用して**[Security]**（セキュリティ設定）→**[Setup password]**（セットアップ パスワード）の順に選択して enter キーを押します。
3. **[New password]**（新しいパスワード）および**[Verify new password]**（新しいパスワードの確認）ボックスにパスワードを入力して f10 キーを押します。
4. **[Security]**（セキュリティ設定）メニューで、矢印キーを使用して**[TPM Embedded Security]**（TPM 内蔵セキュリティ）を選択し、enter キーを押します。
5. **[Embedded Security]**（内蔵セキュリティ）にデバイスが表示されない場合、**[Available]**（利用可能）を選択します。
6. **[Embedded security device state]**（内蔵セキュリティ デバイスの状態）を選択し、**[Enable]**（有効にする）に変更します。
7. f10 キーを押して、Embedded Security の設定への変更を確定します。
8. 設定を保存して[Computer Setup]を終了するには、矢印キーを使用して**[File]**（ファイル）を選択し、**[Save Changes and Exit]**（設定を保存して終了）をクリックします。次に、画面の説明に沿って操作します。

内蔵セキュリティ チップの初期化

内蔵セキュリティの初期化プロセスでは、以下のことを行います。

- 内蔵セキュリティ チップの所有者のパスワードを設定します。これによって、内蔵セキュリティ チップ上のすべての所有者機能へのアクセスが保護されます。
- 緊急リカバリ アーカイブをセットアップします。緊急リカバリ アーカイブとは、すべてのユーザの基本ユーザ キーを再暗号化できるようにするための保護された記憶領域です。

内蔵セキュリティ チップを初期化するには、以下の手順で操作します。

1. タスク バーの右端の通知領域にある[HP ProtectTools Security Manager]（HP ProtectTools セキュリティ マネージャ）アイコンを右クリックして、**[Embedded Security Initialization]**（内蔵セキュリティの初期化）を選択します。

   [HP ProtectTools Embedded Security Initialization Wizard]（HP ProtectTools Embedded Security 初期化ウィザード）が起動します。

2. 画面に表示される説明に沿って操作します。

基本ユーザ アカウントのセットアップ

Embedded Security で基本ユーザ アカウントをセットアップすると、以下のタスクが実行されます。

- 暗号化された情報を保護するための基本ユーザ キーが生成され、その基本ユーザ キーを保護するための基本ユーザ キーのパスワードが設定されます。
- 暗号化されたファイルおよびフォルダを格納するための PSD（Personal Secure Drive）が設定されます。

△ **注意：** 基本ユーザ キーのパスワードは保護しておいてください。このパスワードがないと、暗号化されたデータにアクセスしたり復元したりできなくなります。

基本ユーザ アカウントをセットアップしてユーザ セキュリティ機能を有効にするには、以下の手順で操作します。

1. [Embedded Security User Initialization Wizard]（Embedded Security ユーザ初期化ウィザード）が起動していない場合は、**[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[User Settings]**（ユーザの設定）の順にクリックします。
3. 右側のパネルで、**[Embedded Security Features]**（内蔵セキュリティの機能）の**[Configure]**（設定）をクリックします。

   [Embedded Security User Initialization Wizard]（Embedded Security ユーザ初期化ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。

   注記： セキュリティ保護された電子メールを使用するには、最初に、Embedded Security で作成されたデジタル証明情報を使用するように電子メール クライアントを設定する必要があります。デジタル証明情報が使用できない場合は、証明機関から取得する必要があります。電子メールを設定してデジタル証明情報を取得する手順については、電子メール クライアント ソフトウェアのヘルプを参照してください。

一般的なタスク

基本ユーザ アカウントのセットアップを完了すると、以下のタスクを実行できます。

- ファイルおよびフォルダの暗号化
- 暗号化された電子メールの送受信

PSD（Personal Secure Drive）の使用

PSD のセットアップを完了すると、次回のログオンで、基本ユーザ キーのパスワードを入力するよう要求されます。基本ユーザ キーのパスワードを正しく入力すると、Windows の[エクスプローラ]から直接 PSD にアクセスできます。

ファイルおよびフォルダの暗号化

暗号化ファイルを操作する場合は、以下の規則を考慮してください。

- 暗号化できるファイルおよびフォルダは、NTFS パーティション上のもののみです。FAT パーティション上のファイルおよびフォルダは暗号化できません。
- システム ファイルや圧縮されたファイルは暗号化できません。また、暗号化されたファイルは圧縮できません。
- 一時フォルダは、ハッカーの関心を引く可能性があるため、暗号化するようにしてください。
- ファイルまたはフォルダを初めて暗号化した時、回復ポリシーが自動的にセットアップされます。暗号化証明情報や秘密キーをなくした場合でも、このポリシーによって、回復エージェントを使用して情報の暗号化を解除できるようになります。

ファイルおよびフォルダを暗号化するには、以下の手順で操作します。

1. 暗号化するファイルまたはフォルダを右クリックします。
2. **[Encrypt]**（暗号化）をクリックします。
3. 以下のオプションのどちらかをクリックします。
    - **[Apply changes to this folder only]**（このフォルダにのみ変更を適用する）
    - **[Apply changes to this folder, subfolders, and files]**（このフォルダ、およびサブフォルダとファイルに変更を適用する）
4. **[OK]**をクリックします。

暗号化された電子メールの送受信

Embedded Security では、暗号化された電子メールの送受信を行うことができますが、その手順は電子メールのアクセスに使用しているプログラムによって異なります。詳しくは、Embedded Security ソフトウェアのヘルプおよび使用している電子メール アプリケーション ソフトウェアのヘルプを参照してください。

基本ユーザ キーのパスワードの変更

基本ユーザ キーのパスワードを変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[User Settings]**（ユーザの設定）の順にクリックします。
3. 右側のパネルで、**[Basic User Key password]**（基本ユーザ キーのパスワード）の**[Change]**（変更）をクリックします。
4. 古いパスワードを入力した後、新しいパスワードを設定して確定します。
5. **[OK]**をクリックします。

高度なタスク

バックアップおよび復元

Embedded Security のバックアップ機能では、緊急の場合に復元される証明情報を含むアーカイブが作成されます。

バックアップ ファイルの作成

バックアップ ファイルを作成するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Backup]**（バックアップ）の順にクリックします。
3. 右側のパネルで、**[Backup]**をクリックします。HP Embedded Security for ProtectTools Backup Wizard（HP Embedded Security for ProtectTools バックアップ ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。

バックアップ ファイルからの証明データの復元

バックアップ ファイルからデータを復元するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Backup]**（バックアップ）の順にクリックします。
3. 右側のパネルで、**[Restore]**（復元）をクリックします。HP Embedded Security for ProtectTools Backup Wizard（HP Embedded Security for ProtectTools バックアップ ウィザード）が起動します。
4. 画面に表示される説明に沿って操作します。

所有者のパスワードの変更

所有者のパスワードを変更するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Advanced]**（アドバンス）の順にクリックします。
3. 右側のパネルで、**[Owner Password]**（所有者のパスワード）の**[Change]**（変更）をクリックします。
4. 古い所有者のパスワードを入力した後、新しい所有者のパスワードを設定して確定します。
5. **[OK]**をクリックします。

ユーザ パスワードの再設定

ユーザが忘れたパスワードを管理者に再設定してもらうことができます。詳しくは、ソフトウェアのヘルプを参照してください。

Embedded Security の有効化および無効化

セキュリティ機能を使用しないで操作する場合は、Embedded Security の機能を無効にすることができます。

Embedded Security の機能は、以下の 2 種類のレベルで有効または無効にすることができます。

- 一時的な無効化：このオプションを使用すると、Windows の再起動時に Embedded Security が自動的に再び有効になります。このオプションは、初期設定ですべてのユーザが使用できます。
- 永続的な無効化：このオプションを使用すると、Embedded Security を再び有効にするには所有者のパスワードが必要になります。このオプションは、管理者だけが使用できます。

Embedded Security の永続的な無効化

Embedded Security を永続的に無効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Advanced]**（アドバンス）の順にクリックします。
3. 右側のパネルで、**[Embedded Security]**の**[Disable]**（無効にする）をクリックします。
4. 入力画面で所有者のパスワードを入力して**[OK]**をクリックします。

Embedded Security の永続的な無効化の後の有効化

Embedded Security を永続的に無効にした後で再び有効にするには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。
2. 左側のパネルで、**[Embedded Security]**（内蔵セキュリティ）→**[Advanced]**（アドバンス）の順にクリックします。

3. 右側のパネルで、**[Embedded Security]**の**[Enable]**（有効にする）をクリックします。
4. 入力画面で所有者のパスワードを入力して**[OK]**をクリックします。

移行ウィザードによるキーの移行

移行は、キーや証明情報の管理、復元、転送などを行うことができる、高度な管理者タスクです。

移行について詳しくは、Embedded Security ソフトウェアのヘルプを参照してください。

8　Device Access Manager for HP ProtectTools（一部のモデルのみ）

このセキュリティ ツールは、管理者のみが使用できます。Device Access Manager for HP ProtectTools は、コンピュータ システムに取り付けられたデバイスを不正なアクセスから保護する以下のセキュリティ機能を備えています。

- デバイス アクセスを定義するためにユーザごとに作成されるデバイス プロファイル
- グループ メンバーシップに基づいて許可または拒否可能なデバイス アクセス制御

バックグラウンド サービスの開始

デバイス プロファイルを適用するには、HP ProtectTools Device Locking/Auditing（HP ProtectTools デバイス ロック/検査）バックグラウンド サービスが実行されている必要があります。初めてデバイス プロファイルの適用を試みると、HP ProtectTools セキュリティ マネージャによって、バックグラウンド サービスを開始するかどうかを尋ねるダイアログ ボックスが表示されます。バックグラウンド サービスを開始し、またシステムが起動するたびに自動的に起動するように設定するには、**[Yes]**（はい）をクリックします。

簡易構成

この機能を使用して、以下のクラスのデバイスへのアクセスを拒否できます。

- 管理者以外のユーザによるすべての USB デバイスへのアクセス
- 管理者以外のユーザによるすべてのリムーバブル メディア（フロッピーディスク、USB メモリなど）へのアクセス
- 管理者以外のユーザによるすべての DVD/CD-ROM ドライブへのアクセス
- 管理者以外のユーザによるすべてのシリアル ポートおよびパラレル ポートへのアクセス

管理者以外のすべてのユーザによるデバイス クラスへのアクセスを拒否するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[Simple Configuration]**（簡易構成）の順にクリックします。
3. 右側のパネルで、アクセスを拒否するデバイスのチェック ボックスにチェックを入れます。
4. **[Apply]**（適用）をクリックします。

   注記： バックグラウンド サービスが実行されていない場合は、ここで起動が試みられます。**[Yes]**（はい）をクリックして許可します。

5. **[OK]**をクリックします。

デバイス クラス構成（詳細設定）

特定のユーザまたはユーザ グループによる、特定の種類のデバイスへのアクセスを許可または拒否するための選択項目も利用できます。

ユーザまたはグループの追加

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[Device Class Configuration]**（デバイス クラス構成）の順にクリックします。
3. デバイスの一覧で、設定するデバイス クラスをクリックします。
4. **[Add]**（追加）をクリックします。**[Select Users or Groups]**（ユーザまたはグループの選択）ダイアログ ボックスが表示されます。
5. **[Advanced]**（詳細）→**[Find Now]**（今すぐ検索）の順にクリックして、追加するユーザまたはグループを検索します。
6. 使用可能なユーザおよびグループの一覧に追加するユーザまたはグループをクリックして**[OK]**をクリックします。
7. **[OK]**をクリックします。

ユーザまたはグループの削除

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[Device Class Configuration]**（デバイス クラス構成）の順にクリックします。
3. デバイスの一覧で、設定するデバイス クラスをクリックします。
4. 削除するユーザまたはグループをクリックして**[Remove]**（削除）をクリックします。
5. **[Apply]**（適用）→**[OK]**の順にクリックします。

ユーザまたはグループのアクセス拒否

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[Device Class Configuration]**（デバイス クラス構成）の順にクリックします。
3. デバイスの一覧で、設定するデバイス クラスをクリックします。
4. **[User/Groups]**（ユーザ/グループ）で、アクセスを拒否するユーザまたはグループをクリックします。
5. アクセスを拒否するユーザまたはグループの隣の**[Deny]**（拒否）をクリックします。
6. **[Apply]**（適用）→**[OK]**の順にクリックします。

グループの単一ユーザによるデバイス クラスへのアクセス許可

単一のユーザによるデバイス クラスへのアクセスを許可し、そのユーザのグループのその他のメンバによるアクセスは拒否するように設定できます。

単一のユーザによるアクセスは許可し、グループには許可しないように設定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[Device Class Configuration]**（デバイス クラス構成）の順にクリックします。
3. デバイスの一覧で、設定するデバイス クラスをクリックします。
4. **[User/Groups]**（ユーザ/グループ）で、アクセスを拒否するグループを追加します。
5. アクセスを拒否するグループの隣の**[Deny]**（拒否）をクリックします。
6. 目的のクラスの下のフォルダに移動し、特定のユーザを追加します。**[Allow]**（許可）をクリックして、そのユーザによるアクセスを許可します。
7. **[Apply]**（適用）→**[OK]**の順にクリックします。

グループの単一ユーザによる特定のデバイスへのアクセス許可

単一のユーザによる特定のデバイスへのアクセスを許可し、そのユーザのグループのその他のメンバによる、クラス内のすべてのデバイスへのアクセスは拒否するように設定できます。

特定のデバイスへのアクセスを単一のユーザには許可し、グループには許可しないように設定するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順にクリックします。
2. 左側のパネルで、**[Device Access Manager]**（デバイス アクセス マネージャ）→**[Device Class Configuration]**（デバイス クラス構成）の順にクリックします。
3. デバイスの一覧で、設定するデバイス クラスをクリックして、その下のフォルダに移動します。
4. **[User/Groups]**（ユーザ/グループ）で、アクセスを拒否するグループを追加します。
5. アクセスを拒否するグループの隣の**[Deny]**（拒否）をクリックします。
6. デバイスの一覧で、ユーザによるアクセスを許可する特定のデバイスに移動します。
7. **[Add]**（追加）をクリックします。**[Select Users or Groups]**（ユーザまたはグループの選択）ダイアログ ボックスが表示されます。
8. **[Advanced]**（詳細）をクリックし、**[Find Now]**（今すぐ検索）をクリックして、追加するユーザまたはグループを検索します。
9. アクセスを許可するユーザをクリックして**[OK]**をクリックします。
10. **[Allow]**（許可）をクリックして、そのユーザによるアクセスを許可します。
11. **[Apply]**（適用）→**[OK]**の順にクリックします。

9 トラブルシューティング

Credential Manager for HP ProtectTools

簡単な説明	詳しい説明	解決方法
Credential Manager の [Network Accounts]（ネットワーク アカウント）オプションを使用すると、ユーザはログオン先のドメイン アカウントを選択できる。TPM（Trusted Platform Module）認証が使用されている場合は、このオプションを使用できない。他の認証方法はすべて正しく機能する	TPM 認証を使用している場合、ユーザはローカル コンピュータにのみログオンされます	Credential Manager の[シングルサインオン]ツールを使用すると、ユーザは他のアカウントを認証できるようになります
Credential Manager のインストール後に取り付けたスマート カードおよび USB トークンを Credential Manager で利用できない	スマート カードまたは USB トークンを Credential Manager で使用するには、それらのサポート ソフトウェア（ドライバ、PKCS#11 プロバイダなど）を Credential Manager より先にインストールする必要があります Credential Manager がすでにインストールされている場合は、スマート カードまたはトークンのサポート ソフトウェアをインストールした後、以下の手順で操作します	Credential Manager にログオンします HP ProtectTools セキュリティ マネージャで、**[Credential Manager]**（証明情報マネージャ）→**[Advanced Settings]**（詳細設定）→**[Smart Cards and Tokens]**（スマート カードおよびトークン）タブの順にクリックします。[Local Tokens]（ローカル トークン）の下に、利用可能なトークンの一覧が表示されます [Local Tokens]（ローカル トークン）ノードを右クリックしてポップアップ メニューを開き、[Scan for New Smart Cards and Tokens]（新しいスマート カードおよびトークンのスキャン）を選択します 再起動を求めるメッセージが表示されたら、コンピュータを再起動します
一部のアプリケーションの Web ページでエラーが発生し、ユーザがタスクを実行または完了できなくなる	シングルサインオンの機能無効化パターンによって、一部の Web ベースのアプリケーションが機能を停止し、エラーを報告します。たとえば、Internet Explorer では黄色い三角形の中に**[!]**が表示され、エラーの発生を通知します	Credential Manager シングルサインオンは、すべてのソフトウェアの Web インタフェースをサポートしているわけではありません。シングルサインオンのサポートをオフにすることによって、特定の Web ページに対するシングルサインオンのサポートを無効にしてください。Credential Manager のヘルプ ファイルに含まれている、シングルサインオンに関する詳しいドキュメントを参照してください 特定のアプリケーションで特定のシングルサインオンを無効にできない場合は、HP のサポート窓口にお問い合わせください

簡単な説明	詳しい説明	解決方法
ログオン プロセス中に、**[Browse for Virtual Token]**（仮想トークンの参照）のオプションが表示されない	セキュリティ上のリスクを軽減するために参照のオプションが削除されたため、Credential Manager で、ユーザは登録された仮想トークンの場所を移動できません	参照のオプションは、ユーザ以外の利用者がファイルを削除したり、ファイルの名前を変更したりして Windows を制御できてしまうため、削除されました
権限がある場合でも、ドメイン管理者が Windows パスワードを変更できない	これは、ドメイン管理者がドメインにログオンし、ドメインとローカル コンピュータで管理者の権限をもつアカウントを使用して、ドメイン ID を Credential Manager に登録した後で発生します。ドメイン管理者が、Credential Manager から Windows のパスワードを変更しようとすると、ログオンの失敗を示す次のようなエラー メッセージが表示されます。**[User account restriction]**（ユーザ アカウントの制限）	Credential Manager では、**[Change Windows password]**（Windows パスワードの変更）を使用してドメイン ユーザのアカウント パスワードを変更することはできません。Credential Manager では、ローカル コンピュータのアカウント パスワードのみ変更可能です。ドメイン ユーザは、**[Windows security]**（Windows セキュリティ）の**[Change password]**（パスワードの変更）オプションを使用して自分のパスワードを変更できますが、ドメイン ユーザはローカル コンピュータ上に物理アカウントを持っていないため、Credential Manager はログオンに使用されたパスワードしか変更できません
Credential Manager に、Corel WordPerfect 12 のパスワード GINA との非互換性の問題がある	ユーザが Credential Manager にログオンし、WordPerfect でドキュメントを作成して、パスワード保護を使用して保存した場合、Credential Manager は、パスワード GINA を（手動または自動にかかわらず）検出または認識することができません	HP では、将来の製品の機能強化に生かせるように、回避策を調査中です
Credential Manager が画面の**[Connect]**（接続）ボタンを認識しない	シングルサインオンが再起動されたときに、リモート デスクトップ接続（RDP）のシングルサインオン証明情報が **[Connect]**（接続）に設定されていると、**[Connect]**（接続）の代わりに常に **[Save As]**（名前を付けて保存）が入力されます	HP では、将来の製品の機能強化に生かせるように、回避策を調査中です
ユーザが、TPM で保護されている Credential Manager 証明情報をすべて失う場合がある	TPM モジュールが取り外されたり破損したりすると、TPM が保護する証明情報がすべて失われます	これは仕様です TPM モジュールは、Credential Manager 証明情報を保護するように設計されています。TPM モジュールを取り外す前に、Credential Manager から ID をバックアップしておくことをおすすめします
Windows XP Service Pack 1 を使用している場合のみ、スリープ モードからハイバネーションに移行した後、Credential Manager にログオンできない	システムがハイバネーションやスリープ モードに移行すると、選択されているログオン証明情報の種類（パスワード、指紋、または Java Card）にかかわらず、管理者やユーザは Credential Manager にログオンできなくなり、Windows のログオン画面が表示されたままになります	Windows Update を使用して、Windows を Service Pack 2 にアップデートしてください。この問題の原因について詳しくは、http://www.microsoft.com/japan/にあるマイクロソフト サポート技術情報の文書番号 813301 を参照してください ユーザがログオンするには、Credential Manager を選択してログオンする必要があります。Credential Manager にログオンすると、Windows にログオンして（Windows ログオン オプションの選択が必要になる場合があります）ログオン プロセスを完了するよう要求されます ユーザが最初に Windows にログオンした場合は、手動で Credential Manager にログオンする必要があります
Embedded Security を復元すると、Credential Manager が機能しなくなる	ROM を工場出荷時の設定に復元した後は、Credential Manager が証明書を登録できなくなります	Credential Manager をインストールした後に ROM が工場出荷時の設定に戻されると、Credential Manager は TPM へのアクセスに失敗します

簡単な説明	詳しい説明	解決方法
		TPM 内蔵セキュリティ チップは、f10 [Computer Setup]ユーティリティ、BIOS Configuration、または HP Client Manager を使用して有効にできます。[Computer Setup]を使用してTPM 内蔵セキュリティ チップを有効にするには、以下の手順で操作します 1. コンピュータの電源を入れるか再起動し、画面の左下隅に**[f10=ROM Based Setup]**メッセージが表示されている間に f10 キーを押して、[Computer Setup]を起動します 2. 矢印キーを使用して、**[Security]**（セキュリティ設定）→**[Setup Password]**（セットアップ パスワード）の順に選択します。パスワードを設定します 3. **[Embedded Security Device]**（内蔵セキュリティ デバイス）を選択します 4. 矢印キーを使用して、**[無効]**（Embedded Security Device–Disable）を選択します。矢印キーを使用して、**[有効]**（Embedded Security Device–Enable）に変更します 5. **[Enable]**（有効にする）→**[Save changes and exit]**（設定を保存して終了）の順に選択します HP では、将来のカスタマ ソフトウェア リリースに向けて、解決策を調査中です
セキュリティの**[Restore Identity]**（ID の復元）プロセスで、仮想トークンとの関連付けが失われる	ユーザが ID を復元したとき、Credential Manager で、ログオン画面での仮想トークンの場所との関連付けが失われる場合があります。Credential Manager には仮想トークンが登録されているにもかかわらず、ユーザは関連付けを復元するためにトークンを再登録する必要があります	現在の仕様です ID を保存しないで Credential Manager をアンインストールすると、トークンのシステム（サーバ）の部分が破壊されるため、トークンのクライアントの部分が ID の復元によって復元されたとしても、そのトークンはログオンに使用できなくなります HP では、一時的ではない解決策を調査中です

Embedded Security for HP ProtectTools（一部のモデルのみ）

簡単な説明	詳しい説明	解決方法
PSD（Personal Secure Drive）上のフォルダ、サブフォルダ、およびファイルを暗号化するとエラー メッセージが表示される	ユーザがファイルおよびフォルダを PSD にコピーし、フォルダ/ファイルまたはフォルダ/サブフォルダを暗号化しようとすると、**[Error Applying Attributes]**（属性適用時のエラー）というメッセージが表示されます。C ドライブまたは外付けハードドライブ上では同じファイルを暗号化できます	これは仕様です ファイル/フォルダを PSD に移動すると、これらのファイル/フォルダは自動的に暗号化されます。ファイル/フォルダを二重に暗号化する必要はありません。EFS を使用して PSD 上のファイル/フォルダを二重に暗号化しようとすると、このエラー メッセージが表示されます
マルチブート プラットフォーム環境で別の OS を使用して所有権を得ることができない	ドライブがマルチ OS ブート用にセットアップされている場合でも、所有権を設定できるのは、1 つのオペレーティング システムのプラットフォーム初期化ウィザードからだけです	これはセキュリティを確保するための仕様です
不正な管理者が、暗号化された EFS フォルダの内容の表示、削除、名前の変更、または移動を行うことができる	フォルダを暗号化している場合でも、管理権限がある不正なユーザは、フォルダの内容の表示、削除、または移動を行えます	これは仕様です これは、Embedded Security TPM ではなく EFS の機能です。Embedded Security は、Microsoft EFS ソフトウェアを使用し、EFS がすべての管理者のファイル/フォルダへのアクセス権限を保護します
FAT32 を使用したハードドライブを復元しようとするとき、ユーザに暗号化のオプションが表示されない	FAT32 を使用するハードドライブを復元する場合は、EFS を使用してファイル/フォルダを暗号化するオプションが表示されません	これは仕様です。FAT32 パーティションを含む復元ディスクにはソフトウェアをインストールしないでください Microsoft EFS は NTFS でのみサポートされており、FAT32 では機能しません。これは Microsoft EFS の機能であり、HP ProtectTools ソフトウェアによるものではありません
ユーザがリカバリ アーカイブの XML ファイルを暗号化または削除できる	設計では、このフォルダに ACL は設定されていないため、ユーザがこのファイルを間違えて、または意図的に暗号化または削除することによってアクセス不可能にする可能性があります。このファイルが暗号化または削除されると、だれも TPM（Truted Platform Module）ソフトウェアを使用できなくなります	これは仕様です ユーザは、基本ユーザ キーのバックアップ コピーを保存または更新できるように、緊急アーカイブに対するアクセス権を持っています。リカバリ アーカイブ ファイルを決して暗号化または削除しないようユーザに指示してください
Embedded Security EFS と Symantec Antivirus または McAfee Total Protection との相互通信によって、暗号化/暗号化解除やスキャンの時間が長くなる	暗号化されたファイルは、Symantec Antivirus または McAfee Total Protection のウィルス スキャンと干渉します。Symantec Antivirus または McAfee Total Protection の実行中は、Embedded Security EFS を使用したファイルの暗号化には時間がかかります	Embedded Security EFS ファイルをスキャンするために必要な時間を短縮するために、ユーザはスキャンの前に暗号化パスワードを入力するか、またはスキャンの前に暗号化を解除することができます Embedded Security EFS を使用してデータを暗号化/暗号化解除するために必要な時間を短縮するには、Symantec Antivirus または McAfee Total Protection で [Auto-Protect]（自動保護）を無効にしてください
緊急リカバリ アーカイブをリムーバブル メディアに保存できない	Embedded Security の初期化中、緊急リカバリ アーカイブのパスを作成しているときにユーザがマルチメディア カードまたは SD（Secure Digital）メモリカードを挿入すると、エラー メッセージが表示されます	これは仕様です リムーバブル メディアへのリカバリ アーカイブの保存はサポートされていません。リカバリ アーカイブは、ネットワーク ドライブか、または C ドライブ以外のローカル ドライブに保存できます

簡単な説明	詳しい説明	解決方法
電源の切断によってEmbedded Security の初期化が中断された後、エラーが発生する	Embedded Security チップの初期化中に電源が切断されると、以下の問題が発生します ● [Embedded Security Initialization Wizard]（Embedded Security 初期化ウィザード）を起動しようとしたときに、以下のエラー メッセージが表示されます。**[The Embedded security cannot be initialized since the Embedded Security chip already has an Embedded Security owner.]**（Embedded Security チップにすでに Embedded Security 所有者が設定されているため、Embedded Security を初期化できません。） ● [User Initialization Wizard]（ユーザ初期化ウィザード）を起動しようとしたときに、以下のエラー メッセージが表示されます。**[The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first.]**（Embedded Security が初期化されていません。ウィザードを使用するには、まず Embedded Security を初期化する必要があります。）	電源が切断された後は、以下の手順に沿って回復します **注記：** 特別な指定がない場合、メニューやメニュー項目を選択したり、値を変更したりするには矢印キーを使用します 1. コンピュータを起動または再起動します 2. 画面に「**f10=Setup**」メッセージが表示されたら、f10 キーを押します 3. 該当する言語オプションを選択します 4. enter キーを押します 5. **[Security]**（セキュリティ設定）→**[Embedded Security]**（内蔵セキュリティ）の順に選択します 6. **[Embedded Security Device]**（内蔵セキュリティ デバイス）オプションを**[Enable]**（有効）に設定します 7. f10 キーを押して変更を確定します 8. **[File]**（ファイル）→**[Save Changes and Exit]**（設定を保存して終了）の順に選択します 9. enter キーを押します 10. f10 キーを押して変更を保存し、ユーティリティを終了します
TPM モジュールを有効にした後、[Computer Setup]（f10）ユーティリティのパスワードを削除できる	TPM モジュールを有効にするには、[Computer Setup]（f10）ユーティリティのパスワードが必要です。モジュールを有効にしたら、ユーザはパスワードを削除することができます。これによって、システムに直接アクセスできるユーザが TPM モジュールをリセットできると同時に、データが損失する可能性も発生します	これは仕様です [Computer Setup]（f10）ユーティリティのパスワードは、そのパスワードを知っているユーザのみが削除できます。それでも、[Computer Setup]（f10）ユーティリティのパスワードを常に保護しておくことを強くおすすめします
スタンバイ状態の後にシステムがアクティブになったとき、PSD（Personal Secure Drive）のパスワード ボックスが表示されない	PSD を作成した後にユーザがシステムにログオンすると、TPM から基本ユーザ パスワードを入力するよう求められます。ユーザがパスワードを入力しないうちにシステムのスタンバイが起動された場合、スタンバイから復帰してもパスワード ダイアログ ボックスは表示されません	これは仕様です ユーザがいったんログオフしてからログオンすれば、PSD パスワード ボックスは表示されます
セキュリティ プラットフォーム ポリシーを変更するときにパスワードを要求されない	セキュリティ プラットフォーム ポリシーへのアクセス（マシンとユーザの両方）では、システムの管理権限を持っているユーザは、TPM パスワードの入力を要求されません	これは仕様です TPM ユーザが初期化されている場合でもされていない場合でも、管理者であればセキュリティ プラットフォーム ポリシーを変更できます
証明書を表示すると、信頼されていないものとして表示される	HP ProtectTools をセットアップし、[User Initialization Wizard]（ユーザ初期化ウィザード）を実行した後、ユーザは発行した証明書を表示することができます。ただし、証明書を表示すると、信頼	自己署名の証明書は、信頼されません。正しく設定された企業環境では、EFS の証明書は、オンラインの証明機関が発行し、信頼されます

簡単な説明	詳しい説明	解決方法
	されていないものとして表示されます。インストール ボタンをクリックすることによって、この時点で証明書をインストールできますが、インストールしても信頼される証明書にはなりません	
以下の断続的な暗号化および暗号化解除エラーが発生する。**[The process cannot access the file because it is being used by another process.]**（別のプロセスでファイルが使用されているため、現在のプロセスからはこのファイルにアクセスできません。）	これは、ファイルの暗号化または暗号化解除を行うときに発生する、きわめて断続的なエラーです。そのファイルまたはフォルダがオペレーティング システムやその他のアプリケーションによって処理されていない場合でも、ファイルが別のプロセスによって使用されているために発生します	この問題を解決するには、以下の手順で操作します 1. システムを再起動します 2. ログオフします 3. ログオンしなおします
新しいデータの生成または転送が完了する前にリムーバブル メディアを取り外すと、リムーバブル メディア内のデータが損失する	マルチベイ ハードドライブなどのストレージ メディアを取り外しても、PSD（Personal Secure Drive）は引き続き使用可能と表示され、PSD にデータを追加/変更している間もエラーは生成されません。システムが再起動された後、PSD には、リムーバブル記憶域が使用不可の間に発生したファイル変更が反映されません	データの生成または転送が完了する前に PSD を取り外さないでください。この問題は、ユーザが PSD にアクセスした後、新しいデータの生成または転送が完了する前にハードドライブを取り外した場合にのみ発生します。リムーバブル ハードドライブが存在しないときにユーザが PSD にアクセスしようとすると、**[the device is not ready]**（デバイスの準備ができていません）というエラー メッセージが表示されます
アンインストール中、基本ユーザを初期化しないで管理ツールを開くと、**[Disable]**（無効にする）オプションが使用できず、管理ツールが閉じられるまでアンインストーラの処理が続行されない	ユーザは、TPM を無効にしないでアンインストールするか、または最初に（管理ツールを使用して）TPM を無効にしてからアンインストールするかのどちらかを選択できます。管理ツールにアクセスするには、基本ユーザ キーの初期化が必要です。基本ユーザの初期化が実行されていないと、すべてのオプションがアクセス不可になります **[Click Yes to open Embedded Security Administration tool]**（Embedded Security 管理ツールを開くには[Yes]（はい）をクリックしてください）ダイアログ ボックスで**[Yes]**（はい）をクリックすることによって、管理ツールを開くことを明示的に選択しているため、アンインストールは管理ツールが閉じられるまで行われません。そのダイアログ ボックスで**[No]**（いいえ）をクリックした場合、管理ツールはまったく開かれず、アンインストールの処理が続行されます	管理ツールは TPM チップを無効にするために使用されますが、基本ユーザ キーがすでに初期化されていない限り、そのオプションは使用できません。基本ユーザ キーがまだ初期化されていない場合は、**[OK]**または**[Cancel]**（キャンセル）を選択してアンインストールを続行してください
2 つのユーザ アカウントに PSD を作成し、128 MB のシステム構成でユーザの簡易切り替えを使用した後、断続的にシステムがロックアップする	最小の RAM で簡易切り替えを使用していると、[ようこそ]（ログオン）画面の代わりに黒い画面が表示され、キーボードやマウスの応答がない状態でシステムがロックアップする可能性があります	根本的な原因は、少ないメモリ構成でのタイミングの問題と考えられます 内蔵グラフィックスは、8 MB のメモリが必要な UMA アーキテクチャを採用しているため、ユーザに使用可能なメモリは 120 MB しか残されません。ともにログオンし、ユーザの簡易切り替えを行っている両方のユーザがこの 120 MB を共有すると、このエラーが発生します

簡単な説明	詳しい説明	解決方法
		エラーを回避するには、システムを再起動し、メモリ構成を増やしてください（HP ではセキュリティ モジュール搭載の 128 MB 構成コンピュータを出荷していません）
[access denied]（アクセスが拒否されました）というメッセージが表示され、EFS ユーザ認証（パスワード要求）がタイムアウトする	**[OK]**をクリックするか、またはスタンバイが終了した後、EFS ユーザ認証のパスワード画面が再度開きます	これは仕様です。Microsoft EFS で問題が発生しないように、エラー メッセージを生成するために 30 秒程度のウォッチドッグ タイマーが作成されました
日本語でのセットアップ中に、機能説明が省略されることがある	インストール ウィザード実行時のカスタム セットアップ オプション段階で、機能説明が省略されています	この問題については、将来のリリースで解決します
入力画面にパスワードを入力しなくても、EFS 暗号化が機能する	ユーザ パスワードの入力画面でタイムアウトが可能なため、ファイルまたはフォルダに対して引き続き暗号化を使用できます	暗号化の機能は、Microsoft EFS 暗号化の機能であるため、パスワード認証は必要ありません。暗号化の解除には、ユーザ パスワードの指定が必要になります
[User Initialization Wizard]（ユーザ初期化ウィザード）で電子メールのセキュリティ保護を指定しない場合、またはユーザ ポリシーで電子メールのセキュリティ保護の設定が無効になっている場合でも、電子メールのセキュリティ保護がサポートされる	Embedded Security ソフトウェアやウィザードは、電子メール クライアント（Outlook、Outlook Express、または Netscape）の設定を制御しません	この動作は仕様です。TPM の電子メール設定によって、電子メール クライアントで暗号化の設定を直接編集することは禁止されません。電子メールのセキュリティ保護の使用は、他社製のアプリケーションによって設定および制御されます。HP のウィザードでは、すばやいカスタマイズを可能にするため、3 つの参照アプリケーションにリンクできるようにしています
同じコンピュータまたは以前に初期化したコンピュータで 2 回目の大規模な導入を実行すると、緊急リカバリ ファイルおよび緊急トークン ファイルが上書きされる。新しいファイルは、リカバリに使用できない	以前に初期化された HP ProtectTools Embedded Security システムで大規模な導入を実行すると、XML ファイルが上書きされるため、既存のリカバリ アーカイブおよびリカバリ トークンが使用できなくなります	HP では、XML ファイルの上書きの問題を解決するよう取り組んでおり、将来の SoftPaq で解決策を提供する予定です
Embedded Security でのユーザ復元中に、自動化されたログオン スクリプトが機能しない	このエラーは、ユーザが以下の操作を行った後に発生します ● Embedded Security で、所有者とユーザを初期化する（初期設定の位置の**[マイ ドキュメント]**を使用） ● BIOS で、チップを工場出荷時の設定に戻す ● コンピュータを再起動する ● Embedded Security の復元を開始する。復元処理中、Credential Manager によって、Infineon TPM ユーザ認証へのログオンを自動化するかどうか尋ねられます。**[Yes]**（はい）を選択すると、SPEmRecToken の場所がテキスト ボックスに自動的に表示されます	画面の**[Browse]**（参照）ボタンをクリックして位置を選択してください。復元プロセスが続行されます

簡単な説明	詳しい説明	解決方法
	この位置が正しい場合でも、以下のエラー メッセージが表示されます。**[No Emergency Recovery Token is provided. Select the token location the Emergency Recovery Token should be retrieved from.]**（緊急リカバリ トークンが入力されていません。緊急リカバリ トークンの取得元にするトークン位置を選択してください。）	
ユーザの簡易切り替えの環境で、複数ユーザの PSD が機能しない	このエラーは、複数のユーザが作成され、同じドライブ文字を含む PSD（Personal Secure Drive）が与えられている場合に発生します。PSD がロードされたときにユーザ間でユーザの簡易切り替えを行おうとすると、2 番目のユーザの PSD が使用できなくなります	2 番目のユーザの PSD は、別のドライブ文字を使用するように設定しなおすか、または最初のユーザがログオフした場合にのみ使用可能になります
PSD（Personal Secure Drive）が生成されたハードドライブをフォーマットすると、PSD が無効になり、削除できなくなる	PSD のアイコンは引き続き表示されますが、ユーザが PSD にアクセスしようとすると、**[drive is not accessible]**（ドライブにアクセスできません）というエラー メッセージが表示されます ユーザは PSD を削除できず、以下のメッセージが表示されます。**[your PSD is still in use, please be sure that your PSD contains no open files and is not accessed by another process]**（PSD はまだ使用されています。この PSD に開かれたままのファイルがなく、別のプロセスからもアクセスされていないことを確認してください） この PSD を削除するには、ユーザはシステムをリブートする必要があります。リブートの後、PSD はロードされません	これは仕様です。ユーザが強制的に削除したり、PSD データの保存位置から切断したりしても、Embedded Security PSD ドライブ エミュレーションが機能を続行し、存在しないデータとの通信が途切れるため、エラーが生成されます 解決策：次の再起動後はエミュレーションがロードされないため、ユーザは古い PSD エミュレーションを削除して、新しい PSD を作成できます
ユーザが自動バックアップ アーカイブから復元しているときに内部エラーが検出される	Embedded Security では、自動バックアップ アーカイブから復元するために **[Restore under Backup]**（バックアップの復元）オプションをクリックし、**[SPSystemBackup.xml]**を選択すると、復元ウィザードの実行に失敗して以下のエラー メッセージが表示されます。**[The selected Backup Archive does not match the restore reason. Please select another archive and continue.]**（選択されたバックアップ アーカイブは復元の理由に一致しません。別のアーカイブを選択して続行してください。）	SpBackupArchive.xml が必要なときに **[SpSystemBackup.xml]**を選択すると、Embedded Security ウィザードの実行に失敗して以下のメッセージが表示されます。**[An internal Embedded Security error has been detected.]**（Embedded Security の内部エラーが検出されました。） 必要な理由に一致する正しい XML ファイルを選択する必要があります プロセスは設計どおりに正しく機能していますが、Embedded Security 内部エラー メッセージが明確でないため、より適切なメッセージを表示する必要があります。HP は、将来の製品で改善するよう取り組んでいます
セキュリティ システムで、複数のユーザでの復元エラーが発生する	復元プロセス中、管理者が復元するユーザを選択した場合、選択されなかったユーザが後で復元を試みてもキーを復元できません。**[decryption process failed]**（暗号化の解除プロセスが失敗しました）というエラー メッセージが表示されます	選択されなかったユーザは、初期設定による次回の日次バックアップが実行される前に、TPM をリセットし、復元プロセスを実行して、すべてのユーザを選択することによって復元できます。自動化されたバックアップが実行された場合は、復元されなかったユーザが上書きされ、それらのユーザのデータは失われます。新しいシステム バックアップ データが保存されると、選択されなかった以前のユーザは復元できなくなります

簡単な説明	詳しい説明	解決方法
		また、ユーザがシステム全体のバックアップを復元することも必要です。アーカイブ バックアップは個別に復元できます
システム ROM を初期設定に戻すと、TPM が表示されなくなる	システム ROM を初期設定に戻すと、Windows が TPM を認識できなくなります。これより、セキュリティ ソフトウェアが正しく動作しなくなり、TPM の暗号化データにアクセスできなくなります	以下の手順に沿って、BIOS で TPM を再表示します [Computer Setup]（f10）ユーティリティを開き、**[Security]**（セキュリティ設定）→**[Device security]**（デバイス セキュリティ）の順に選択して、フィールドを**[Hidden]**（非表示）から**[Available]**（利用可能）に変更します
マップされたドライブで自動バックアップが機能しない	管理者が Embedded Security で自動バックアップをセットアップすると、Windows XP の**[スタート]**→[コントロール パネル]→[パフォーマンスとメンテナンス]→**[タスク]**→**[タスク名]**にエントリが作成されます。この[タスク名]は、バックアップを実行するためのアクセス権として NT AUTHORITY\SYSTEM を使用するように設定されています。この設定はどのローカル ドライブに対しても正しく機能します 管理者が、自動バックアップでマップされたドライブに保存されるように設定すると、NT AUTHORITY\SYSTEM にはマップされたドライブを使用する権限がないため、プロセスは失敗します 自動バックアップをログオン時に実行するようにスケジュールが設定されている場合は、Embedded Security の TNA アイコンに以下のメッセージが表示されます。**[The Backup Archive location is currently not accessible. Click here if you want to backup to a temporary archive until the Backup Archive is accessible again.]**（バックアップ アーカイブの場所に現在アクセスできません。バックアップ アーカイブが再びアクセス可能になるまで一時的なアーカイブにバックアップする場合は、ここをクリックしてください。）ただし、自動バックアップが特定の時間にスケジュール設定されている場合は、失敗の通知が表示されることなくバックアップが失敗します	この問題を回避するには、NT AUTHORITY\SYSTEM を[コンピュータ名]\[管理者名]に変更してください。これは、スケジュールされたタスクが手動で作成される場合の初期設定です HP では、[コンピュータ名]\[管理者名]を含む初期設定を備える製品を将来リリースできるよう取り組みを進めています
Embedded Security の GUI で Embedded Security を一時的に無効にできない	最新の 4.0 ソフトウェアは、HP Notebook 1.1B への実装と、HP Desktop 1.2 への実装をサポートすることを目的にして設計されました 無効化のためのこのオプションは、TPM 1.1 プラットフォームのソフトウェア インタフェースでもサポートされています	この問題については、将来のリリースで対応します

Device Access Manager for HP ProtectTools

簡単な説明	詳しい説明	解決方法
Device Access Manager 内でユーザがデバイスへのアクセスを拒否されたが、これらのデバイスは引き続きアクセス可能である	ユーザによるデバイスへのアクセスを拒否するために、Device Access Manager 内では簡易構成やデバイス クラス構成が使用されてきました。アクセスを拒否されたにもかかわらず、ユーザは引き続きデバイスにアクセスできます	HP ProtectTools デバイス ロック サービスが開始していることを確認してください 管理者権限のあるユーザとしてログインし、**[コントロール パネル]**→[管理ツール]→[サービス]の順に選択します。**[サービス]**ウィンドウで、**[HP ProtectTools Device Locking/Auditing]**（HP ProtectTools デバイス ロック/検査）サービスを見つけます。このサービスが開始されおり、スタートアップの種類が**[自動]**であることを確認してください
ユーザがデバイスへの予期しないアクセスを許可されているか、またはユーザがデバイスへのアクセスを予期せず拒否される	Device Access Manager は、一部のデバイスへのアクセスを拒否し、その他のデバイスへのアクセスを許可するために使用されてきました。ユーザがシステムを使用中に、Device Access Manager によって拒否されていると思っていたデバイスにアクセスできたり、Device Access Manager によって許可されていると思っていたデバイスへのアクセスを拒否されたりすることがあります	ユーザのデバイス設定の調査には、Device Access Manager 内のデバイス クラス構成を使用してください **[Security Manager]**（セキュリティ マネージャ）→**[Device Access Manager]**→**[Device Class Configuration]**（デバイス クラス構成）の順に選択します。[Device Class]（デバイス クラス）ツリーの各レベルを展開し、ユーザに該当する設定を確認します。そのユーザに対して設定されている[Deny]（拒否）アクセス権、またはそのユーザがメンバになっている Windows グループ（たとえば、Users、Administrators など）があるかどうかを確認してください
許可と拒否のどちらが優先されるか	デバイス クラス構成内では、以下の構成が設定されています ● [Allow]（許可）アクセス権は、ある Windows グループ（たとえば、BUILTIN\Administrators）に許可されています。一方、[Deny]（拒否）アクセス権は、デバイス クラス階層内の同じレベル（たとえば、DVD/CD-ROM ドライブ）にある別の Windows グループ（たとえば、BUILTIN\Users）に許可されています あるユーザがこの両方のグループのメンバ（たとえば管理者）である場合は、どちらが優先されますか	このユーザはデバイスへのアクセスを拒否されます。拒否は許可より優先されます アクセスは、Windows でデバイスに対する有効なアクセス権が決定される方法に従って拒否されます。あるグループが拒否され、別のグループが許可されていますが、ユーザはこの両方のグループのメンバです。アクセスの拒否はアクセスの許可より優先されるため、このユーザは拒否されます 回避策の 1 つは、DVD/CD-ROM ドライブのレベルにある Users グループを拒否し、DVD/CD-ROM ドライブより低いレベルにある Administrators グループを許可することです 別の回避策として、DVD/CD へのアクセスを許可するためと、DVD/CD へのアクセスを拒否するために別々の、特定の Windows グループを作成する方法もあります。それから、該当するグループに特定のユーザを追加します

その他

影響を受けるソフトウェアの簡単な説明	詳しい説明	解決方法
セキュリティ マネージャ：以下の警告が表示される。**[The security application can not be installed until the HP Protect Tools Security Manager is installed.]**（HP ProtectTools セキュリティ マネージャがインストールされるまで、セキュリティ アプリケーションをインストールできません。）	Embedded Security、Java Card Security、指紋認証などのセキュリティ アプリケーションはすべて、セキュリティ マネージャ インタフェースの拡張可能なプラグインです。HP が承認しているセキュリティ プラグインをロードするには、先にセキュリティ マネージャをインストールしておく必要があります	セキュリティ プラグインをインストールする前に、セキュリティ マネージャ ソフトウェアをインストールしておく必要があります
Broadcom に対応した TPM を含むモデルの TPM ファームウェア アップデート ユーティリティ：HP のサポート Web サイトから提供されたツールで **[ownership required]**（オーナーシップが必要）と表示される	これは、Broadcom に対応した TPM を含むモデルの TPM ファームウェア ユーティリティの予期された動作です ユーザは、公認キー（EK）がある場合もない場合も、このファームウェア アップグレード ツールを使用して、ファームウェアをアップグレードできます。EK がない場合は、ファームウェア アップグレードの実行に権限は必要ありません EK がある場合は、アップグレードに所有者の権限が必要なため、TPM 所有者が存在する必要があります。アップグレードが正常に行われた後、プラットフォームを再起動して、新しいファームウェアを有効にする必要があります BIOS TPM が工場出荷時の状態にリセットされると、所有権は削除され、Embedded Security ソフトウェアのプラットフォームとユーザの初期化のためのウィザードの設定が完了するまで、アップデート機能を使用できません 注記： ファームウェアのアップデートを実行した後は、必ず再起動してください。ファームウェア バージョンは、再起動が完了するまで正しく識別されません	1. Embedded Security ソフトウェアを再インストールします 2. [Platform and User Configuration Wizard]（プラットフォームおよびユーザ設定ウィザード）を実行します 3. 以下の手順に沿って、システムに Microsoft .NET Framework 1.1 がインストールされていることを確認します a. **[スタート]**をクリックします b. **[コントロール パネル]**をクリックします c. **[プログラムの追加と削除]**をクリックします d. **[Microsoft .NET Framework 1.1]**が表示されていることを確認します 4. 以下の手順に沿って、ハードウェアとソフトウェアの構成を確認します a. **[スタート]**をクリックします b. **[すべてのプログラム]**をクリックします c. **[HP ProtectTools セキュリティ マネージャ]**をクリックします d. ツリー メニューから**[Embedded Security]**を選択します e. **[More Details]**（詳細）をクリックします。システムは、以下のような構成になっている必要があります • Product version（製品バージョン）= V4.0.1 • Embedded Security State（内蔵セキュリティの状態）: Chip State（チップの状態）＝ Enabled（有効）、Owner State（所有者の状態）＝ Initialized（初期化済み）、User State（ユーザの状態）＝ Initialized（初期化済み）

影響を受けるソフトウェアの簡単な説明	詳しい説明	解決方法
		● Component Info（コンポーネント情報）: TCG Spec. Version（TCG 仕様バージョン）= 1.2 ● Vendor（ベンダ） = Broadcom Corporation ● FW Version（FW バージョン）= 2.18（または、それ以上） ● TPM デバイス ドライバ ライブラリ バージョン 2.0.0.9（またはそれ以上） 5. ファームウェア バージョンが 2.18 でない場合は、TPM ファームウェアをダウンロードしてアップデートします。TPM ファームウェアの SoftPaq は、HP の Web サイト http://www.hp.com/jp/からダウンロードできます
HP ProtectTools セキュリティ マネージャ : セキュリティ マネージャ インタフェースを閉じたとき、エラーが返されることがある	すべてのプラグイン アプリケーションのロードが終了する前に、セキュリティ マネージャを閉じようとして画面右上の閉じるボタンを使用すると、エラーが発生することがあります（12 回に 1 回ぐらいの割合）	これは、セキュリティ マネージャを終了および再起動するときに、そのタイミングがプラグイン サービス ロード時間の影響を受けることに関連しています。PTHOST.exe は、他のアプリケーション（プラグイン）を収納するシェルであるため、プラグインのロード時間（サービス）の終了能力の影響を受けます。この問題の根本原因は、プラグインのロード終了にかかる時間が経過していないのにシェルが閉じられたことです セキュリティ マネージャがサービス ロード メッセージ（[Security Manager]（セキュリティ マネージャ）ウィンドウの一番上に表示される）をすべて出力し、左の列にすべてのプラグインが一覧表示されるまで待ちます。エラーを回避するため、プラグインをロードするときは時間を十分にとってください
HP ProtectTools : 無制限のアクセスや制御されていない管理権限によってセキュリティ上のリスクが生じる	クライアント コンピュータへのアクセスが無制限の場合、以下のような多くのリスクが生じる可能性があります ● PSD の削除 ● ユーザ設定への悪意のある変更 ● セキュリティ ポリシーや機能の無効化	管理者が最善の方法でエンドユーザの権限を制限し、ユーザのアクセスを制限することをおすすめします 不正なユーザに管理権限を与えないでください
BIOS と OS の Embedded Security パスワードが同期していない	新しいパスワードを BIOS Embedded Security パスワードとして確定しない場合、BIOS の Embedded Security パスワードは、f10 BIOS によって元の内蔵セキュリティ パスワードに戻されます	これは仕様です。このパスワードは、OS の基本ユーザ パスワードを変更し、BIOS Embedded Security パスワードの入力画面で認証すれば、再同期されます
BIOS の TPM ブート前認証を有効にした後、1 人のユーザしかシステムにログオンできない	TPM BIOS の PIN は、ユーザ設定を初期化する最初のユーザに関連付けられます。コンピュータに複数のユーザが存在する場合は、基本的に、最初のユーザが管理者になります。他のユーザがログオンするには、最初のユーザがそのユーザに自分の TPM ユーザ PIN を通知する必要があります	これは仕様です。ユーザの IT 部門が適切なセキュリティ ポリシーに従ってセキュリティ ソリューションを展開すること、さらに BIOS 管理者パスワードはシステム レベルで保護されるように必ず IT 管理者が設定することをおすすめします

影響を受けるソフトウェアの簡単な説明	詳しい説明	解決方法
TPM を工場出荷時設定に戻した後に TPM ブート前認証を機能させるには、ユーザは自分の PIN を変更する必要がある	設定を戻した後に TPM の BIOS 認証を機能させるには、ユーザは自分の PIN を変更するか、または別のユーザを作成してユーザ設定を初期化する必要があります。TPM の BIOS 認証を機能させるためのオプションはありません	これは仕様です。工場出荷時設定に戻すと基本ユーザ キーが消去されます。基本ユーザ キーを再び初期化するには、ユーザは自分のユーザ PIN を変更するか、または新しいユーザを作成する必要があります
Embedded Security の **[Reset to Factory Settings]**（工場出荷時の設定に戻します）を使用しても、**[Power-on authentication support]**（起動時の認証サポート）が初期設定にならない	コンピュータ セットアップ（F10）ユーティリティで、Embedded Security デバイス オプションの**[Reset to Factory Settings]**（工場出荷時の設定に戻します）を使用しても、**[起動時の認証サポート]**オプションは工場出荷時の設定にリセットされません。初期設定では、**[Power-on authentication support]**（起動時の認証サポート）は、**[Disable]**（無効）に設定されます	**[Reset to Factory Settings]**（工場出荷時の設定に戻します）オプションによって内蔵セキュリティ デバイスが無効になり、それによって、他の Embedded Security オプション（**[Power-on authentication support]**（起動時の認証サポート）を含む）が非表示になります。ただし、内蔵セキュリティ デバイスを再度有効にすると、**[Power-on authentication support]**（起動時の認証サポート）が有効のままになります HP では解決策に向けた取り組みを進めており、将来の Web ベース ROM の SoftPaq で提供する予定です
起動処理中、セキュリティ電源投入時認証が BIOS パスワードと重複している	電源投入時認証では、ユーザは TPM パスワードを使用してシステムにログオンするよう求められますが、**[f10]**キーを押して BIOS にアクセスすると、読み取りのアクセス権のみを許可されます	BIOS への書き込みを可能にするには、電源投入時認証のウィンドウで、TPM パスワードの代わりに BIOS パスワードを入力する必要があります
所有者のパスワードを変更した後、[Computer Setup]を介して BIOS によって古いパスワードと新しいパスワードの両方の入力が求められる	Windows の Embedded Security ソフトウェアで所有者のパスワードを変更した後、[Computer Setup]を介して BIOS によって古いパスワードと新しいパスワードの両方の入力が求められます	これは仕様です。オペレーティング システムの起動後に、BIOS が TPM と通信できず、TPM のパスフレーズを確認できないことが原因です

用語集

[Send Securely]（安全に送信）ボタン： [Microsoft Outlook]の電子メール メッセージのツールバーに表示されるソフトウェア ボタン。このボタンをクリックすると、[Microsoft Outlook]の電子メール メッセージに対する署名や暗号化ができます。

[Sign and Encrypt]（署名と暗号化）ボタン： Microsoft Office アプリケーションのツールバーに表示されるソフトウェア ボタン。このボタンをクリックすると、Microsoft Office ドキュメントに対する署名、暗号化、または暗号化の解除ができます。

Automatic Technology Manager（ATM）： ネットワーク管理者がシステムを BIOS レベルでリモート管理できます。

BIOS セキュリティ モード： 有効にすると、ユーザ認証に Java Card および有効な PIN の使用が必要になる、Java Card セキュリティでの設定。

BIOS プロファイル： 他のアカウントに保存および適用できる、BIOS 設定値の集合。

BIOS 管理者パスワード： [Computer Setup]のセットアップ パスワード。

Chat History Viewer： 暗号化されたチャット履歴セッションの検索と表示ができる、[Privacy Manager Chat]コンポーネント。

Drive Encryption キー復元サービス： SafeBoot の[Recovery Service]。暗号化キーのコピーを保存します。パスワードを忘れたためローカルのバックアップ キーにアクセスできない場合には、このコピーを使用することでコンピュータにアクセスできます。バックアップ キーへのオンライン アクセスを設定するサービスを持つアカウントを作成する必要があります。

Drive Encryption のログオン画面： Windows が起動する前に表示されるログオン画面。ユーザは、Windows のユーザ名およびパスワード、または Java Card の PIN を入力する必要があります。ほとんどの場合、Drive Encryption のログオン画面で正しい情報を入力すれば、Windows のログオン画面で再度ログインすることなく、直接 Windows にアクセスできます。

DriveLock： ハードドライブをユーザにリンクして、コンピュータの起動時にユーザに正しい DriveLock パスワードの入力を要求するセキュリティ機能。

HP SpareKey： Drive Encryption キーのバックアップ コピー。

ID： HP ProtectTools Credential Manager 内で、特定のユーザのアカウントまたはプロファイルのように処理される、証明情報と設定の集合。

Java Card：　コンピュータに挿入するリムーバブル カード。ログオン用の識別情報が保存されています。Drive Encryption のログオン画面で Java Card を使用してログインするには、Java Card を挿入し、ユーザ名および Java Card の PIN を入力する必要があります。

PSD（Personal Secure Drive）：　機密情報を保護するための記憶領域を提供する機能。

Privacy Manager Certificate：　電子メール メッセージおよび Microsoft Office ドキュメントに対する署名や暗号化など、暗号の演算に使用するたびに認証が必要なデジタル証明書。

SATA デバイス モード：　コンピュータと大容量ストレージ デバイス（ハードドライブやオプティカル ドライブなど）の間のデータ転送モード。

TPM（Trusted Platform Module）内蔵セキュリティ チップ（一部のモデルのみ）：　HP ProtectTools 内蔵セキュリティ チップの一般的な呼び方。TPM では、ホスト システムに固有の情報（暗号化キー、デジタル署名、パスワードなど）が格納され、ユーザではなくコンピュータが認証されます。TPM を使用すると、物理的な盗難や外部のハッカーによる攻撃によってコンピュータ上の情報が危険にさらされるリスクを最小限に抑えることができます。

Trusted Contact の一覧：　Trusted Contact の一覧。

Trusted Contact の受信者：　Trusted Contact になるための招待を受け取った人物。

Trusted Contact への招待状：　Trusted Contact になることを依頼するために送信された電子メール。

Trusted Contact 宛てに封印：　電子メールにデジタル署名を付加した上で暗号化し、選択したセキュリティ ログオン方法による認証の後に送信する作業。

Trusted Contact：　Trusted Contact への招待を承認した人物。

TXT：　Trusted Execution Technology の略語。

USB トークン：　ユーザに関する識別情報が格納されているセキュリティ デバイス。Java Card や指紋認証システムと同様に、所有者をコンピュータに対して認証するために使用されます。

Windows ユーザ アカウント：　ネットワークまたは個別のコンピュータへのログオンを承認された個人のプロファイル。

Windows 管理者：　アクセス権を変更し、他のユーザを管理するすべての権限を持つユーザ。

暗号化サービス プロバイダ（CSP）：　明確なインタフェースを使用して特定の暗号化関数を実行するための暗号化アルゴリズムの提供者またはライブラリ。

暗号化の解除：　暗号化されたデータを平文に変換するための、暗号法で使用される手順。

暗号化ファイル システム（EFS）：　選択されたフォルダ内のすべてのファイルおよびサブフォルダを暗号化するシステム。

暗号化：　権限のない受信者がデータを解読できないように平文を暗号文に変換するための、暗号法で使用されるアルゴリズムなどの手順。データの暗号化にはさまざまな種類があり、ネットワーク セキュリティの基礎として使用されます。一般的な暗号化には、データ暗号化規格（DES）や公開キー暗号があります。

暗号法：　特定の個人のみが解読できるように、データを暗号化および暗号化解除する手法。

管理者：　「Windows 管理者」を参照してください。

キーの組み合わせ：　特定のキーの組み合わせ。ctrl ＋ alt ＋ s キーなどを押すと、自動シュレッドが開始されます。

緊急リカバリ アーカイブ： 他のプラットフォームの所有者キーを使用して基本ユーザ キーを再暗号化できる、保護された記憶領域。

公開キー基盤（PKI）： 証明情報および暗号化キーを作成、使用、および管理するためのインタフェースを定義する規格。

自動 DriveLock： DriveLock パスワードが生成され、TPM 内蔵セキュリティ チップによって保護されるようにするセキュリティ機能。起動時にユーザが正しい TPM 基本ユーザ キーのパスワードを入力し、それが TPM 内蔵セキュリティ チップによって認証されると、BIOS によってそのユーザ用のハードドライブの保護が解除されます。

手動シュレッド： 単一のフォルダやファイルまたは選択されている複数のフォルダやファイルに対して、自動シュレッド スケジュールを無視して実行されるシュレッド。

シングルサインオン： 認証情報を格納し、パスワード認証が必要なインターネットおよび Windows アプリケーションに Credential Manager を使用してアクセスできるようにする機能。

シンプル削除： Windows のフォルダやファイルの参照情報の削除。空き領域ブリーチを実行しても、フォルダやファイルの内容をわからなくするデータをフォルダやファイルに上書きしないかぎり、そのフォルダやファイルの内容はハードドライブ上に残ります。

シュレッド サイクル： 各フォルダやファイルでシュレッド アルゴリズムを実行する回数。選択したシュレッド サイクルの回数が多いほど、コンピュータのセキュリティは高くなります。

シュレッド プロファイル： あらかじめ指定されている消去方法とフォルダやファイルの一覧。

シュレッド： フォルダやファイルに含まれるデータの内容をわからなくするアルゴリズムの実行。

スマート カード： 所有者に関する識別情報が格納されている、サイズと形状がクレジット カードに似た小さなハードウェア。所有者をコンピュータに対して認証するために使用されます。

セキュリティ ログオン方法： コンピュータへのログインに使用される方法。

チャット履歴： チャット セッションでの双方の会話の記録が含まれている、暗号化されたファイル。

デジタル署名： 資料の送信者を証明し、署名された後にファイルが変更されていないことを証明するファイルとともに送信されるデータ。

デジタル証明書： デジタル証明書の所有者の身元と、デジタル情報の署名に使用される電子キーのペアとを結びつけることによって、個人または企業の身元を証明する電子的な信用証明書。

電源投入時認証： Java Card、セキュリティ チップ、パスワードなど、コンピュータの起動時に何らかの形式の認証を要求するセキュリティ機能。

ドメイン： ネットワークの一部であり、共通のディレクトリ データベースを共有するコンピュータの集合。ドメインには一意の名前が付けられ、各ドメインには一連の共通の規則および手順が設定されます。

トークン： 「セキュリティ ログオン方法」を参照してください。

認証機関： 公開キー基盤の運営に必要な証明書を発行するサービス。

証明情報： ユーザが認証プロセスで特定のタスクに対する適格性を証明するための方法。

ネットワーク アカウント： ローカル コンピュータ上、ワークグループ内、またはドメイン上の Windows ユーザまたは管理者のアカウント。

バイオメトリック（生体認証）： 指紋などの身体的な特徴を使用してユーザを識別する認証証明のカテゴリ。

フォルダやファイル： 個人の情報やファイル、履歴や Web 関連のデータなどを含むデータ コンポーネント。ハードドライブ上に存在します。

ユーザ： Drive Encryption に登録された人。管理者以外のユーザは、Drive Encryption での権限が制限されています。管理者以外のユーザが実行できる操作は、登録（管理者の許可がある場合）とログインのみです。

リブート： コンピュータを再起動するプロセス。

移行： Privacy Manager Certificate および Trusted Contact を管理、復元、および転送する作業。

仮想トークン： Java Card やカード リーダーとよく似た働きをするセキュリティ機能。このトークンは、コンピュータのハードドライブ上か、Windows レジストリ内のどちらかに保存されます。仮想トークンでログオンすると、認証を完了するためにユーザ PIN の入力を要求されます。

空き領域ブリーチ： 削除されたフォルダやファイルにランダムなデータを安全に上書きして、削除されたフォルダやファイルの元の内容をわからなくすること。

厳重なセキュリティ： 電源投入時パスワード、管理者パスワード、およびその他の形態の、電源投入時認証に対する保護機能を強化する、BIOS Configuration にあるセキュリティ機能。

公開： ユーザが 1 つ以上のチャット履歴セッションの暗号化を解除して、Contact Screen Name を平文で表示し、セッションを表示できるようにする作業。

自動シュレッド： ユーザが File Sanitizer for HP ProtectTools で設定したスケジュールに従って実行されるシュレッド。

署名欄： デジタル署名を表示するためのプレースホルダ。ドキュメントに署名すると、署名者の名前と確認方法が表示されます。署名日と署名者のタイトルも表示できます。

信頼できる IM 通信： 信頼できる送信者から Trusted Contact に宛てて、信頼できるメッセージを送信する通信セッション。

信頼できるメッセージ： 信頼できる送信者から Trusted Contact に宛てて、信頼できるメッセージを送信する通信セッション。

信頼できる送信者： 署名および暗号化した電子メールや Microsoft Office ドキュメントを送信する Trusted Contact。

推奨する署名者： ドキュメントに署名欄を追加するために[Microsoft Word]または[Microsoft Excel]ドキュメントの所有者が指名したユーザ。

認証： ユーザがタスクの実行（コンピュータへのアクセス、特定のプログラムの設定変更、セキュリティ保護されたデータの表示など）を承認されているかどうかを確認するプロセス。

廃止パスワード： ユーザがデジタル証明書を要求する際に作成されるパスワード。このパスワードは、ユーザがデジタル証明書を廃止する場合に必要です。これによって、ユーザ自身のみが証明書を廃止できるようになります。

有効化： Drive Encryption の機能にアクセスする前に完了する必要があるタスク。Drive Encryption は、HP ProtectTools セキュリティ マネージャのセットアップ ウィザードを使用して有効にします。管理者のみが Drive Encryption を有効にすることができます。有効化プロセスは、ソフトウェアの有効化、ドライブの暗号化、ユーザ アカウントの作成、およびリムーバブル ストレージ デバイス上の初期バックアップ暗号化キーの作成で構成されます。

索引

S

T

W

あ

お

か

き

こ

さ

し

せ